## Some of the things you will learn in THE CODEBREAKERS

- How secret Japanese messages were decoded in Washington hours before Pearl Harbor.
- How German codebreakers helped usher in the Russian Revolution.
- How John F. Kennedy escaped capture in the Pacific because the Japanese failed to solve a simple cipher.
- How codebreaking determined a presidential election, convicted an underworld syndicate head, won the battle of Midway, led to cruel Allied defeats in North Africa, and broke up a vast Nazi spy ring.
- How one American became the world's most famous codebreaker, and another became the world's greatest.
- How codes and codebreakers operate today within the secret agencies of the U.S. and Russia.
- And incredibly much more.

"For many evenings of gripping reading, no better choice can be made than this book."
—*Christian Science Monitor*

# THE
# Codebreakers

## The Story of Secret Writing

**By DAVID KAHN**
*(abridged by the author)*

A SIGNET BOOK from
**NEW AMERICAN LIBRARV**
TIMES MIRROR

Copyright © 1967, 1973 by David Kahn
All rights reserved.
No part of this book may be reproduced or transmitted
in any form or by any means, electronic or mechanical,
including photocopying, recording or by any information
storage and retrieval system, without permission in writing
from the publisher. For information address
The Macmillan Company, 866 Third Avenue, New York,
New York 10022.
Library of Congress Catalog Card Number: 63-16109
Crown copyright is acknowledged for the following illustrations
from Great Britain's Public Record Office:
S.P. 53/18, no. 55, the Phelippes forgery,
and P.R.O. 31/11/11, the Bergenroth reconstruction.
Published by arrangement with The Macmillan Company
FIRST PRINTING SECOND PRINTING THIRD PRINTING FOURTH PRINTING FIFTH PRINTING SIXTH PRINTING SEVENTH PRINTING
EIGHTH PRINTING NINTH PRINTING TENTH PRINTING
SIGNET TRADEMARK: REG. TJ.S. PAT. OFF. AND FOREIGN COUNTRIES
REGISTERED TRADEMARK---MARCA REGISTBADA
HECHO EN CHICAGO, U.S.A.
SIGNET, SIGNET CLASSICS, SIGNETTE, MENTOR AND PLUME BOOKS
*are published by The New American Library, Inc.,*

*1301 Avenue of the Americas, New York, New York 10019*
FIRST PRINTING, FEBRUARY, 1973
PRINTED IN THE UNITED STATES OF AMERICA

*To my Parents*
*and my Grandmother*

## Contents

*A Note on the Abridged Version*
*Preface*
*A Few Words*
*1.* One Day of Magic: I
2. One Day of Magic: II
3. The First 3,000 Years
4. The Rise of the West
5. On the Origin of a Species
6. The Era of the Black Chambers
7. The Contribution of the Dilettantes
8. Room 40
9. A War of Intercepts
10. Two Americans
11. Secrecy for Sale
12. Duel in the Ether: I
13. Duel in the Ether: II
14. Censors, Scramblers, and Spies
15. The Scrutable Orientals
16. PYCCKAJI Kranrojioras
17. N.S.A.
18. Heterogeneous Impulses
19. Ciphers in the Past Tense
20. The Anatomy of Cryptology
*Suggestions for Further Reading*
*Index*

## A Note on the Abridged Version

MANY PEOPLE have urged me to put out a paperback edition of *The Codebreakers.* Here it is.

It comprises about a third of the original. This was as big as the publishers and I could make it and still keep the price within reason.

In cutting the book, I retained mainly stories about how codebreaking has affected history, particularly in World War II, and major names and stages in the history of cryptology. I eliminated all source notes and most of the technical matter, as well as material peripheral to strict codebreaking such as biographies, the invention of secondary cipher systems, and miscellaneous uses of various systems.

I had no space for new material, but I did correct the errors reported to me and updated a few items. The chapters have been slightly rearranged.

Readers wanting to know more about a specific point should consult the text and notes of the original.

If any reader wishes to offer any corrections or to tell me of his own experiences in this field, I would be very grateful if he would send them to me.

—D.K.

*Windsor Gate*
*Great Neck, New York*

# Preface

CODEBREAKING is the most important form of secret intelligence in the world today. It produces much more and much more trustworthy information than spies, and this intelligence exerts great influence upon the policies of governments. Yet it has never had a chronicler.

It badly needs one. It has been estimated that cryptanalysis saved a year of war in the Pacific, yet the histories give it but passing mention. Churchill's great history of World War II has been cleaned of every single reference to Allied communications intelligence except one (and that based on the American Pearl Harbor investigation), although Britain thought it vital enough to assign 30,000 people to the work. The intelligence history of World War II has never been written. All this gives a distorted view of why things happened. Furthermore, cryptology itself can benefit, like other spheres of human endeavor, from knowing its major trends, its great men, its errors made and lessons learned.

I have tried in this book to write a serious history of cryptology. It is primarily a report to the public on the important role that cryptology has played, but it may also orient cryptology with regard to its past and alert historians to the sub rosa influence of cryptanalysis. The book seeks to cover the entire history of cryptology. My goal has been twofold: to narrate the development of the various methods of making and breaking codes and ciphers, and to tell how these methods have affected men.

When I began this book, I, like other well-informed amateurs, knew about all that had been published on the history of cryptology in books on the subject. How little we really knew! Neither we nor any professionals realized that many valuable articles lurked in scholarly journals, or had induced any cryptanalysts to tell their stories for publication, or had tapped the vast treasuries of documentary material, or had tried to take a long view and ask some questions that now appear basic. I believe it to be true that, from the point of view of the material previously published in books on cryptology, what is new in this book is 85 to 90 per cent.

Yet it is not exhaustive. A foolish secrecy still clothes much of World War II cryptology—though I believe the outlines of the achievements are known—and to tell just that story in full would require a book the size of this. Even in, say, the 18th century, the unexplored manuscript material is very great.

Nor is this a textbook. I have sketched a few methods of solution. For some readers even this will be too much; them I advise skip this material. They will not have a full understanding of what is going on, but that will not cripple their comprehension of the stories. For readers who want more detail on these methods, I recommend, in the rear of this book, some other works and membership in the American Cryptogram Association.

In my writing, I have tried to adhere to two principles. One was to use primary sources as much as possible. Often it could not be done any other way, since nothing had been published on a particular matter. The other principle was to try to make certain that I did not give cryptology sole and total credit for winning a battle or making possible a diplomatic coup or whatever happened if, as was usual, other factors played a role. Narratives which make it appear as if every event in history turned upon the subject under discussion are not history but journalism. They are especially prevalent in spy stories, and cryptology is not immune. The only other book-length attempt to survey the history of cryptology, the late Fletcher Pratt's *Secret and Urgent,* published in 1939, suffers from a severe case of this special pleading. Pratt writes thrillingly—perhaps for that very reason—but his failure to consider the other factors, together with his errors and omissions, his false generalizations based on no evidence, and his unfortunate predilection for inventing facts vitiate his work as any kind of a history. (Finding this out was disillusioning, for it was this book, borrowed from the Great Neck Library, that interested me in cryptology.) I think that although trying to balance the story with the other factors may detract a little from the immediate thrill, it charges it with authenticity and hence makes for long-lasting interest: for this is how things really happened.

In the same vein, I have not made up any conversations, and my speculations about things not a matter of record have been marked as such in the notes in the full-length version. I have documented all important facts, except that in a few cases I have had to respect the wishes of my sources for anonymity.

The original publisher submitted the manuscript to the Department of Defense on March 4, 1966, which requested three minor deletions—to all of which I acceded—before releasing the manuscript for publication.

DAVID KAHN

*Windsor Gate*
*Great Neck, New York*
*Paris*

## A Few Words

EVERY TRADE has its vocabulary. That of cryptology is simple, but even so a familiarity with its terms facilitates understanding. A glossary may also serve as a handy reference. The definitions in this one are informal and ostensive. Exceptions are ignored and the host of minor terms are not defined—the text covers these when they come up.

The **plaintext** is the message that will be put into secret form. Usually the plaintext is in the native tongue of the communicators. The message may be hidden in two basic ways. The methods of **steganography** conceal the very existence of the message. Among them are invisible inks and microdots and arrangements in which, for example, the first letter of each word in an apparently innocuous text spells out the real message. (When steganography is applied to electrical communications, such as a method that transmits a long radio message in a single short spurt, it is called **transmission security.)** The methods of **cryptography,** on the other hand, do not conceal the presence of a secret message but render it unintelligible to outsiders by various transformations of the plaintext.

Two basic transformations exist. In **transposition,** the letters of the plaintext are jumbled; their normal order is disarranged. To shuffle *secret* into ETCRSE is a transposition. In **substitution,** the letters of the plaintext are replaced by other letters, or by numbers or symbols. Thus *secret* might become 19 5 3 18 5 20, or XIWOXY in a more complicated system. In transposition, the letters retain their identities— the two e's of *secret* are still present in ETCRSE—but they lose their positions, while in substitution the letters retain their positions but lose their identities. Transposition and substitution may be combined.

Substitution systems are much more diverse and important than transposition systems. They rest on the concept of the **cipher alphabet.** This is the list of equivalents used to transform the plaintext into the secret form. A sample cipher alphabet might be:

| | |
|---|---|
| *plaintext letters* | abcdefghijklm |
| *cipher letters* | LBQACSRDTOFVM |
| *plaintext letters* | nopqrstuvwxyz |
| *cipher letters* | HWIJXGKYUNZEP |

This graphically indicates that the letters of the plaintext are to be replaced by the cipher letters beneath them, and vice versa. Thus, *enemy* would become CHCME, and swc would reduce to *foe.* A set of such correspondences is still called a "cipher alphabet" if the plaintext letters are in mixed order, or even if they are missing, because cipher letters always imply plaintext letters.

Sometimes such an alphabet will provide multiple substitutes for a letter. Thus plaintext *e,* for example, instead of always being replaced by, say, 16, will be replaced by any one of the figures 16, 74, 35, 21. These alternates are called **homophones.** Sometimes a cipher alphabet will include symbols that mean nothing and are intended to confuse interceptors; these are called **nulls.**

As long as only one cipher alphabet is in use, as above, the system is called **monoalpbabetic.** When, however, two or more cipher alphabets are employed in some kind of prearranged pattern, the system becomes **polyalphabetic.** A simple form of polyalphabetic substitution would be to add another cipher alphabet under the one given above and then to use the two in rotation, the first alphabet for the first plaintext letter, the second for the second, the first again for the third plaintext letter, the second for the fourth, and so on. Modern cipher machines produce polyalphabetic ciphers that employ millions of cipher alphabets.

Among the systems of substitution, **code** is distinguished from **cipher.** A code consists of thousands of words, phrases, letters, and syllables with the **codewords or code-numbers** (or, more generally, the **codegroups)** that replace these plaintext elements.

| *plaintext* | *codeword* |
|---|---|
| emplacing | DVAP |
| employ | DVBO |
| en- | DVCN |
| enable | DVDM |
| enabled | DVEL |

enabled to DVFK

This means, of course, that DVDM replaces *enable.* If the plaintext and the code elements both run in alphabetical or numerical order, as above, the code is a **one-part code,** because a single book serves for both en- and decoding. If, however, the code equivalents stand in mixed order opposite their plaintext elements, like this

| *Plaintext* | *codenumber* |
|---|---|
| shield (for) | 51648 |
| shielded | 07510 |
| shielding | 10983 |
| shift(s) | 43144 |
| ship | 35732 |
| ships | 10762 |

the code is a **two-part code,** because a second section, in which the code elements are in regular order, is required for decoding:

| *codenumber* | *plaintext* |
|---|---|
| 10980 | was not |
| 10981 | spontaneous (ly) |
| 10983 | shielding |
| 10986 | April 13 |
| 10988 | withdrawn from |
| 10990 | acknowledge |

In a sense, a code comprises a gigantic cipher alphabet, in which the basic plaintext unit is the word or the phrase; syllables and letters are supplied mainly to spell out words not present in the code. In ciphers, on the other hand, the basic unit is the letter, sometimes the letter-pair **(digraph or bigram),** very rarely larger groups of letters **(polygrams).** The substitution and transposition systems illustrated above are ciphers. There is no sharp theoretical dividing line between codes and ciphers; the latter shade into the former as they grow larger. But in modern practice the differences are usually quite marked. Sometimes the two are distinguished by saying that ciphers operate on plaintext units of regular length (all single letters or all groups of, say, three letters), whereas codes operate on plaintext groups of variable length (words, phrases, individual letters, etc.). A more penetrating and useful distinction is that code operates on linguistic entities, dividing its raw material into meaningful elements like words and syllables, where as cipher does not—cipher will split the *t* from the *h* in *the,* for example.

For 450 years, from about 1400 to about 1850, a system that was half a code and half a cipher dominated cryptography. It usually had a separate cipher alphabet with homophones and a codelike list of names, words, and syllables. This list, originally just of names, gave the system its name: **nomenclator.** Even though late in its life some nomenclators grew larger than some modern codes, such systems are still called "nomenclators" if they fall within this historical period. An odd characteristic is that nomenclators were always written on large folded sheets of paper, whereas modern codes are almost invariably in book or booklet form. The **commercial code** is a code used in business primarily to save on cable tolls; though some are compiled for private firms, many others are sold to the public and therefore provide no real secrecy.

Most ciphers employ a key, which specifies such things as the arrangement of letters within a cipher alphabet, or the pattern of shuffling in a transposition, or the settings on a cipher machine. If a word or phrase or number serves as the key, it is naturally called the **keyword or keyphrase or keynumber.** Keys exist within a **general system** and control that system's variable elements. For example, if a polyalphabetic cipher provides 26 cipher alphabets, a keyword might define the half dozen or so that are to be used in a particular message.

Codewords or codenumbers can be subjected to transposition or substitution just like any other group of letters or numbers—the transforming processes do not ask that the texts given to them be intelligible. Code that has not yet undergone such a process—called **superencipherment** —or which has been

deciphered from it is called **placode,** a shortening of "plain code." Code that has been transformed is called **encicode,** from "enciphered code."

To pass a plaintext through these transformations is to **encipher** or **encode** it, as the case may be. What comes out of the transformation is the **ciphertext** or the **codetext.** The final secret message, wrapped up and sent, is the **cryptogram.** (The term "ciphertext" emphasizes the result of encipherment more, while "cryptogram" emphasizes the fact of transmission more; it is analogous to "telegram.") To **decipher** or **decode** is for the persons legitimately possessing the key and system to reverse the transformations and bare the original message. It contrasts with **cryptanalyze,** in which persons who do not possess the key or system— a third party, the "enemy"—break down or solve the cryptogram. The difference is, of course, crucial. Before about 1920, when the word **cryptanalysis** was coined to mean the methods of breaking codes and ciphers, "decipher" and "decode" served in both senses (and occasionally still do), and in quotations where they are used in the sense of solve, they are retained if they will not confuse. Sometimes cryptanalysis is called **codebreaking;** this includes solving ciphers. The original intelligible text that emerges from either decipherment or cryptanalysis is again called **plaintext.** Messages sent without encipherment are **cleartext** or **in clear,** though they are sometimes called **in plain language.**

**Cryptology** is the science that embraces cryptography and cryptanalysis, but the term "cryptology" sometimes loosely designates the entire dual field of both rendering signals secure and extracting information from them. This broader field has grown to include many new areas; it encompasses, for example, means to deprive the enemy of information obtainable by studying the traffic patterns of radio messages, and means of obtaining information from radar emissions. An outline of this larger field, with its opposing parts placed opposite one another, and with a few of the methods of each part given in parentheses, would be:

| SIGNAL SECURITY | SIGNAL INTELLIGENCE |
|---|---|
| Communication Security | Communication Intelligence |
| Steganography (invisible inks, open codes, messages in hollow heels) and Transmission Security (spurt radio systems) | Interception and Direction-Finding |
| Traffic Security (call-sign changes, dummy messages, radio silence) | Traffic Analysis (direction-finding fixes, message-flow studies, radio-fingerprinting) |
| Cryptography (codes and ciphers, ciphony, cifax) | Cryptanalysis |
| Electronic Security | Electronic Intelligence |
| Emission Security (shifting of radar frequencies) | Electronic Reconnaissance (eavesdropping on radar emissions) |
| Counter-Countermeasures ("looking-through" jammed radar) | Countermeasures (jamming, false radar echoes) |

This book employs certain typographic conventions for simplicity and economy. Plaintext is always set lower case; when it occurs in the running text (as opposed to its occurrence in the diagrams), it is also in *italics.* Cipher-text or codetext is set in SMALL CAPS in the text, keys in LARGE CAPS. They are distinguished in the diagrams by labels. Cleartext and translations of foreign-language plaintext are in roman within quotation marks. The sound of a letter or syllable or word, as distinguished from its written form, is placed within diagonals, according to the convention widely followed in linguistics; thus /t/ refers to the unvoiced stop normally represented by that letter and not to the graphic symbol *t*.

D. K.

## 1. One Day of Magic: I

AT 1:28 on the morning of December 7, 1941, the big ear of the Navy's radio station on Bainbridge Island near Seattle trembled to vibrations in

the ether. A message was coming through on the Tokyo-Washington circuit. It was addressed to the Japanese embassy, and Bainbridge reached up and snared it as it flashed overhead. The message was short, and its radiotelegraph transmission took only nine minutes. Bainbridge had it all by 1:37.

The station's personnel punched the intercepted message on a teletype tape, dialed a number on the teletypewriter exchange, and when the connection had been made, fed the tape into a mechanical transmitter that gobbled it up at 60 words per minute.

The intercept reappeared on a page-printer in Room 1649 of the Navy Department building on Constitution Avenue in Washington, D.C. What went on in this room, tucked for security's sake at the end of the first deck's sixth wing, was one of the most closely guarded secrets of the American government. For it was in here—and in a similar War Department room in the Munitions Building next door—that the United States peered into the most confidential thoughts and plans of its possible enemies by shredding the coded wrappings of their dispatches.

Room 1649 housed OP-20-GY, the cryptanalytic section of the Navy's cryptologic organization, OP-20-G. The page-printer stood beside the desk of the GY watch officer. It rapped out the intercept in an original and a carbon copy on yellow and pink teletype paper just like news on a city room wireservice ticker. The watch officer, Lieutenant (j.g.) Francis M. Brotherhood, U.S.N.R., a curly-haired, brown-eyed six-footer, saw immediately from indicators that the message bore for the guidance of Japanese code clerks that it was in the top Japanese cryptographic system.

This was an extremely complicated machine cipher which American cryptanalysts called PURPLE. Led by William F. Friedman, Chief Cryptanalyst of the Army Signal Corps, a team of codebreakers had solved Japan's enciphered dispatches, deduced the nature of the mechanism that would effect those letter transformations, and painstakingly built up an apparatus that cryptographically duplicated the Japanese machine. The Signal Corps had then constructed several additional PURPLE machines, using a hodgepodge of manufactured parts, and had given one to the Navy. Its three components rested now on a table in Room 1649: an electric typewriter for input; the cryptographic assembly proper, consisting of a plugboard, four electric coding rings, and associated wires and switches, set on a wooden frame; and a printing unit for output. To this precious contraption, worth quite literally more than its weight in gold, Brotherhood carried the intercept.

He flicked the switches to the key of December 7. This was a rearrangement, according to a pattern ascertained months ago, of the key of December 1, which OP-20-QY had recovered. Brotherhood typed

out the coded message. Electric impulses raced through the maze of wires, reversing the intricate enciphering process. In a few minutes, he had the plaintext before him.

It was in Japanese. Brotherhood had taken some of the orientation courses in that difficult language that the Navy gave to assist its cryptanalysts. He was in no sense a translator, however, and none was on duty next door in OP-20-GZ, the translating section. He put a red priority sticker on the decode and hand-carried it to the Signal Intelligence Service, the Army counterpart of OP-20-O, where he knew that a translator was on overnight duty. Leaving it there, he returned to OP-20-G. By now it was after 5 a.m. in Washington—the message having lost three hours as it passed through three time zones in crossing the continent.

The S.I.S translator rendered the Japanse as: "Will the Ambassador please submit to the United States Government (if possible to the Secretary of State) our reply to the United States at 1:00 p.m. on the 7th, your time." The —"reply" referred to had been transmitted by Tokyo in 14 parts over the past 18½ hours, and Brotherhood had only recently decrypted the 14th part on the PURPLE machine. It had come out in the English in which Tokyo had framed it, and its ominous final sentence read: "The Japanese Government regrets to have to notify hereby the American Government that in view of the attitude of the American Government it cannot but consider that it is impossible to reach an agreement through further negotiations." Brotherhood had set it by for distribution early in the morning.

The translation of the message directing delivery at one o'clock had not yet come back from S.I.S. when Brotherhood was relieved at 7 a.m., and he told his relief, Lieutenant (j.g.) Alfred V. Pering, about it. Half an hour later, Lieutenant Commander Alwin D. Kramer, the Japanese-language expert who headed GZ and delivered the intercepts, arrived. He saw at once that the all-important conclusion of the long Japanese diplomatic note had come in since he had distributed the 13 previous parts the night before. He prepared a smooth copy from the rough decode and had his clerical assistant, Chief Yeoman H. L. Bryant, type up the usual 14 copies. Twelve of these were distributed by Kramer and his opposite number in S.I.S. to the President, the secretaries of State, War, and Navy, and a handful of top-ranking Army and Navy officers. The two others were file copies. This decode was part of a whole series of Japanese intercepts, which had long ago been given a collective codename, partly for security, partly for ease of reference, by a previous director of naval intelligence, Rear Admiral Walter S. Anderson. Inspired, no doubt, by the mysterious daily production of the information and by the aura of sorcery and the occult that has always enveloped cryptology, he called it MAGIC.

When Bryant had finished, Kramer sent S.I.S. its seven copies, and at 8 o'clock took a copy to his superior, Captain Arthur H. McCollum, head of the Far Eastern Section of the Office of Naval Intelligence.

**From: Tokyo**

**To: Washington**

**December 7, 1941**

**Purple (Urgent - Very Important)**

**#907. To be handled in goverment code.**

**Re: my #902[a].**

**Will the Ambaagador please submit to the United States Government (If possible to the Secretary of State) our reply to the United States at 1:00 p.m. on the 7th, your time.**

**a - JD-1:7143 - text of Japanese reply.**

MAGIC'S *solution of the Japanese one o'clock delivery message*

He then busied himself in his office, working on intercepted traffic, until 9:30, when he left to deliver the 14th part of Tokyo's reply to Admiral Harold F. Stark, the Chief of Naval Operations, to the White House, and to Frank Knox, the Secretary of the Navy. Knox was meeting at 10 a.m. that Sunday morning in the State Department with Secretary of War Henry L. Stimson and Secretary of State Cordell Hull to discuss the critical nature of the American negotiations with Japan, which, they knew from the previous 13 parts, had virtually reached an impasse. Kramer returned to his office about 10:20, where the translation of the message referring to the one o'clock delivery had arrived from S.I.S. while he was on his rounds.

Its import crashed in upon him at once. It called for the rupture of Japan's negotiations with the United States by a certain deadline. The hour set for the Japanese ambassadors to deliver the notification—1 p.m. on a Sunday—was highly unusual. And, as Kramer had quickly ascertained by drawing a navigator's time circle, 1 p.m. in Washington meant 7:30 a.m. in Hawaii and a couple of hours before dawn in the tense Far East around Malaya, which Japan had been threatening with ships and troops.

Kramer immediately directed Bryant to insert the one o'clock message into the reddish-brown looseleaf cardboard folders in which the MAGIC intercepts were bound. He included several other intercepts, adding one

at the last minute, then slipped the folders into the leather briefcases, zipped these shut, and snapped their padlocks. Within ten minutes he was on his way.

He went first to Admiral Stark's office, where a conference was in session, and indicated to McCollum, who took the intercept from him, the nature of the message and the significance of its timing. McCollum grasped it at once and disappeared into Stark's office. Kramer wheeled and hurried down the passageway. He emerged from the Navy Department building and turned right on Constitution Avenue, heading for the meeting in the State Department four blocks away. The urgency of the situation washed over him again, and he began to move on the double.

This moment, with Kramer running through the empty streets of Washington bearing his crucial intercept, an hour before sleepy code clerks at the Japanese embassy had even deciphered it and an hour before the Japanese planes roared off the carrier flight decks on their treacherous mission, is perhaps the finest hour in the history of cryptology. Kramer ran while an unconcerned nation slept late, ignored aggression in the hope that it would go away, begged the hollow gods of isolationism for peace, and refused to entertain—except humorously—the possibility that the little yellow men of Japan would dare attack the mighty United States. The American cryptanalytic organization swept through this miasma of apathy to reach a peak of alertness and accomplishment unmatched on that day of infamy by any other agency in the United States. That is its great achievement, and its glory. Kramer's sprint symbolizes it.

Why, then, did it not prevent Pearl Harbor? Because Japan never sent any message saying anything like "We will attack Pearl Harbor." It was therefore impossible for the cryptanalysts to solve one. Messages had been intercepted and read in plenty dealing with Japanese interest in warship movements into and out of Pearl Harbor, but these were evaluated by responsible intelligence officers as on a par with the many messages dealing with American warships in other ports and the Panama Canal. The causes of the Pearl Harbor disaster are many and complex, but no one has ever laid any of whatever blame there may be at the doors of OP-20-G or S.I.S. On the contrary, the Congressional committee that investigated the attack praised them for fulfilling their duty in a manner that "merits the highest commendation."

As the climax of war rushed near, the two agencies— together the most efficient and successful codebreaking organization that had ever existed—scaled heights of accomplishment greater than any they had ever achieved. The Congressional committee, seeking the responsibility

for the disaster, exposed their activity on almost a minute-by-minute basis. For the first time in history, it photographed in fine-grained detail the operation of a modern code-breaking organization at a moment of crisis. This is that film. It depicts OP-20-G and S.I.S. in the 24 hours preceding the Pearl Harbor attack, with the events of the past as prologue. It is the story of one day of MAGIC.

The two American cryptanalytic agencies had not sprung full-blown into being like Athena from the brow of Zeus. The Navy had been solving at least the simpler Japanese diplomatic and naval codes in Rooms 1649 and 2646 on the "deck" above since the 1920s. The Army's cryptanalytical work during the 1920s was centered in the so-called American Black Chamber under Herbert O. Yardley, who had organized it as a cryptologic section of military intelligence in World War I. It was maintained in secrecy in New York jointly by the War and State departments, and perhaps its greatest achievement was its 1920 solution of Japanese diplomatic codes. At the same time, the Army's cryptologic research and code-compiling functions were handled by William Friedman, then as later a civilian employee of the Signal Corps. In 1929, Henry L. Stimson, then Secretary of State, withdrew State Department support from the Black Chamber on ethical grounds, dissolving it. The Army decided to consolidate and enlarge its codemaking and codebreaking activities. Accordingly, it created the Signal Intelligence Service, with Friedman as chief, and, in 1930, hired three junior cryptanalysts and two clerks.

The following year, a Japanese general suddenly occupied Manchuria and set up a puppet Manchu emperor, and the government of the island empire of Nippon fell into the hands of the militarists. Their avarice for power, their desire to enrich their have-not nation, their hatred for white Occidental civilization, started them on a decade-long march of conquest. They withdrew from the League of Nations. They began beefing up the Army. They denounced the naval disarmament treaties and began an almost frantic ship-building race. Nor did they neglect, as part of their war-making capital, their cryptographic assets. In 1934, their Navy purchased a commercial German cipher machine called the Enigma; that same year, the Foreign Office adopted it, and it evolved into the most secret Japanese system of cryptography. A variety of other cryptosystems supplemented it. The War, Navy, and Foreign ministries shared the superenciphered numerical HATO code for intercommunication. Each ministry also had its own hierarchy of codes. The Foreign Office, for example, employed four main systems, each for a specific level of security, as well as some additional miscellaneous ones.

Meanwhile, the modern-style shoguns speared into defenseless China, sank the American gunboat *Panay,* raped Nanking, molested American

hospitals and missions in China, and raged at American embargoes on oil and steel scrap. It became increasingly evident that Nippon's march of aggression would eventually collide with American rectitude. The mounting curve of tension was matched by the rising output of the American cryptanalytic agencies. A trickle of MAGIC in 1936 had become a stream in 1940. Credit for this belongs largely to Major General Joseph O. Mauborgne, who became Chief Signal Officer in October, 1937.

Mauborgne had long been interested in cryptology. In 1914, as a young first lieutenant, he achieved the first recorded solution of a cipher known as the Playfair, then used by the British as their field cipher. He described his technique in a 19-page pamphlet that was the first publication on cryptology issued by the United States government. In World War I, he put together several cryptographic elements to create the only theoretically unbreakable cipher, and promoted the first automatic cipher machine, with which the unbreakable cipher was associated.

When he became head of the Signal Corps, he immediately set about augmenting the important cryptanalytic activities. He established the S.I.S. as an independent division reporting directly to him, enlarged its functions, set up branches, started correspondence courses, added intercept facilities, increased its budget, and put on more men. In 1939, when war broke out in Europe, S.I.S. was the first agency in the War Department to receive more funds, personnel, and space. Perhaps most important of all, Mauborgne's intense interest inspired his men to outstanding accomplishments. More and more codes were broken, and as the international situation stimulated an increasing flow of intercepts, the MAGIC intelligence approached flood stage.

Mauborgne retired in September, 1941, leaving an expanded organization running with smooth efficiency. By then the Japanese had completed the basic outline for a dawn attack on Pearl Harbor. The plan had been conceived in the fertile brain of Admiral Isoroku Yamamoto, Commander-in-Chief Combined Fleet, Imperial Japanese Navy. Early in the year, he had ordered a study of the operation, contending that "If we have war with the United States, we will have no hope of winning unless the United States fleet in Hawaiian waters can be destroyed." By May 1941, studies had shown the feasibility of a surprise air attack, statistics had been gathered, and operational planning was under way.

In the middle of that month, the U.S. Navy took an important step in the radio intelligence field. It detached a 43-year-old lieutenant commander from his intelligence berth aboard U.S.S. *Indianapolis* and assigned him to reorganize and strengthen the radio intelligence unit at Pearl Harbor. The officer was Joseph John Rochefort, the only man in the Navy with expertise in three closely related and urgently needed fields: cryptanalysis, radio, and the Japanese language. Rochefort, who had begun his career as an enlisted man, had headed the Navy's

cryptographic section from 1925 to 1927. Two years later, a married man with a child, he was sent, because of his outstanding abilities, as a language student to Japan, a hard post to which ordinarily only bachelor officers were sent. This three-year tour was followed by half a year in naval intelligence; most of the next eight years were spent at sea.

Finally, in June of 1941, Rochefort took over the command of what was then known as the Radio Unit of the 14th Naval District in Hawaii. To disguise its functions he renamed it the Combat Intelligence Unit. His mission was to find out, through communications intelligence, as much as possible about the dispositions and operations of the Japanese Navy. To this end he was to cryptanalyze all minor and one of the two major Japanese naval crypto-systems.

His chief target was the flag officers' system, the Japanese Navy's most difficult and the one in which it encased its most secret information. From about 1926 to the end of November, 1940, previous editions had provided the U.S. Navy with much of its information on the Japanese Navy. But the new version—a four-character code with a transposition superencipherment—was stoutly resisting the best efforts of the Navy's most skilled cryptanalysts, and Rochefort was urged to concentrate on it. The other major system, the main fleet cryptographic system, the most widely used, comprised a code with five digit code-numbers to which were added a key of other numbers to complicate the system. The Navy called it the "five numeral system," or, more formally, JN25b—the JN for "Japanese Navy," the 25 an identifying number, the b for the second (and current) edition. Navy cryptanalytic units in Washington and the Philippines were working on this code. Rochefort's unit did not attack this but did attack the eight or ten lesser codes dealing with personnel, engineering, administration, weather, fleet exercises.

But cryptanalysis was only part of the unit's task. The great majority of its 100 officers and men worked on two other aspects of radio intelligence—direction-finding and traffic analysis.

Direction-finding locates radio transmitters. Since radio signals are heard best when the receiver points at the transmitter, sensitive antennas can find the direction from which a signal is coming by swinging until they hear it at its loudest. If two direction-finders take bearings like that on a signal and a control center draws the lines of direction on a map, the point at which they cross marks the position of the transmitter. Such a fix can tell quite precisely where, for example, a ship is operating. Successive fixes can plot its course and speed.

To exploit this source of information, the Navy in 1937 established the Mid-Pacific Strategic Direction-Finder Net. By 1941, high-frequency direction-finders curved in a gigantic arc from Cavite in the Philippines

through Guam, Samoa, Midway, and Hawaii to Dutch Harbor, Alaska. The 60 or 70 officers and men who staffed these outposts reported their bearings to Hawaii, where Rochefort's unit translated them into fixes. For example, on October 16, the ship with call-sign KUNA 1 was located at 10.7 degrees north latitude, 166.7 degrees east longitude—or within Japan's mandated islands.

These findings did not serve merely to keep an eye on the day-to-day locations of Japanese warships. They also formed the basis of the even more fruitful technique of traffic analysis. Traffic analysis deduces the lines of command of military or naval forces by ascertaining which radios talk to which. And since military operations are usually accompanied by an increase in communications, traffic analysis can infer the imminence of such operations by watching the volume of traffic. When combined with direction-finding, it can often approximate the where and when of a planned movement.

Radio intelligence thus maintains a long-range, invisible, and continuous surveillance of fleet movements and organization, providing a wealth of information at a low cost. Of course it has its limitations. A change of the call-signs of radio transmitters can hinder it. The sending of fictitious messages can befuddle it. Radio silences can deafen it. But it cannot be wholly prevented except by unacceptable restrictions on communications. Hence the Navy relied increasingly on it for its information on Japanese naval activities as security tightened in Japan during 1941, and almost exclusively after July, when the President's trade-freezing order deprived the Navy of all visual observations of Japanese ships not on the China coast.

It was in July that a Japanese tactic set up a radio pattern that was later to deceive the Combat Intelligence Unit. The Nipponese militarists had decided to take advantage of France's defeat and occupy French Indochina. The Naval preparations for the successful grab were clearly indicated in the radio traffic, which went through the usual three stages that preceded major Japanese operations. First appeared a heavy flurry of messages. The Commander-in-Chief Combined Fleet busily originated traffic, talking with many commands to the south, thereby indicating the probable direction of his advance. Then came a realignment of forces. In the lingo of the tranalysis people, certain chickens (fleet units) no longer had their old mothers (fleet commanders). Call-sign NOTA 4, which usually communicated with OYO 8, now talked mostly with ORU 6. Accompanying this was a considerable confusion in the routing of messages, with frequent retransmissions caused by the regrouping: Admiral z not here; try Second Fleet. Then followed the third phase: radio silence. The task force was now under way. Messages would be addressed to it, but none would emanate from it.

During all this, however, not only were no messages heard from the

aircraft carriers, none were sent to them, either. This blank condition exceeded radio silence, which suppresses traffic in only one direction—from the mobile force—not in both. American intelligence reasoned that the carriers were standing by in home waters as a covering force in case of counterattack, and that communications both to and from them were not heard because they were being sent out by short-range, low-powered transmissions that died away before reaching American receivers. Such a blank condition had obtained in a similar tactical situation in February. American intelligence had drawn the same conclusions then and had been proven right. Events soon confirmed the July assessment as well. Twice, then, a complete blank of carrier communications combined with indications of a strong southward thrust had meant the presence of the carriers in Empire waters. But what happened in February and July was not necessarily what would happen in December.

During the summer and fall of 1941, the pressure of events molded America's two cryptanalytic agencies closer and closer to the form they were to have on December 7. The Signal Intelligence Service, which had 181 officers, enlisted men, and civilians in Washington and 150 at intercept stations in the field on Pearl Harbor Day, had been headed since March by Lieutenant Colonel Rex W. Minckler, a career Signal Corps officer. Friedman served as his chief technical assistant. S.I.S. comprised the Signal Intelligence School, which trained Regular Army and Reserve officers in cryptology, the 2nd Signal Service Company, which staffed the intercept posts, and four Washington sections of the S.I.S. proper: the A, or administrative, which also operated the tabulating machinery; the B, or cryptanalytic; the c, or cryptographic, which prepared new U.S. Army systems, studied the current systems for security, and monitored Army traffic for security violations; and the D, or laboratory, which concocted secret inks and tested suspected documents.

The B section, under Major Harold S. Doud, a West Point graduate, had as its mission the solution of the military and diplomatic systems not only of Japan but of other countries. In this it apparently achieved at least a fair success, though no Japanese military systems—the chief of which was a code employing four-digit codenum-bers—were readable by December 7 because of a paucity of material. Doud's technical assistant was a civilian, Frank B. Rowlett, one of the three original junior cryptanalysts hired in 1930. The military man in charge of Japanese diplomatic solutions was Major Eric Svensson.

The Navy's official designation of OP-20-G indicated that the agency was the G section of the 20th division of OPNAV, the Office of the Chief of Naval Operations, the Navy's headquarters establishment. The 20th division was the Office of Naval Communications, and the G section was

the Communication Security Section. This carefully chosen name masked its cryptanalytic activities, though its duties did include U. S. Navy cryptography.

Its chief was Commander Laurence F. Safford, 48, a tall, blond Annapolis graduate who was the Navy's chief expert in cryptology. In January, 1924, he had become the officer in charge of the newly created research desk in the Navy's Code and Signal Section. Here he founded the Navy's communication-intelligence organization. After sea duty from 1926 to 1929, he returned to cryptologic activities for three more years, when sea duty was again made necessary by the "Manchu" laws, which required officers of the Army and Navy to serve in the field or at sea to win promotion. He took command of OP-20-G in 1936. One of his principal accomplishments before the outbreak of war was the establishment of the Mid-Pacific Strategic Direction-Finder Net and of a similar net for the Atlantic, where it was to play a role of immense importance in the Battle of the Atlantic against the U-boats.

Safford's organization enjoyed broad cryptologic functions. It printed new editions of codes and ciphers and distributed them, and contracted with manufacturers for cipher machines. It developed new systems for the Navy. It comprehended such subsections as GI, which wrote reports based on radio intelligence from the field units, and GL, a record-keeping and historical-research group. But its main interest centered on cryptanalysis.

This activity was distributed among units in Washington, Hawaii, and the Philippines. Only Washington attacked foreign diplomatic systems and naval codes used in the Atlantic theater (primarily German). Rochefort had primary responsibility for the Japanese naval systems. The Philippines chipped away at JN25 and did some diplomatic deciphering, with keys provided by Washington. That unit, which like Rochefort's was attached for administrative purposes to the local naval district (the 16th), was installed in a tunnel of the island fortress of Corregidor. It was equipped with 26 radio receivers, apparatus for intercepting both high- and low-speed transmissions, a directionfinder, and tabulating machinery. Lieutenant Rudolph J. Fabian, 33, an Annapolis graduate who had had three years of radio intelligence experience in Washington and the Philippines, commanded. The 7 officers and 19 men in his cryptanalytic group exchanged possible recoveries of JN25b codegroups with Washington and with a British group in Singapore; each group also had a liaison man with the other.

Of the Navy's total radio-intelligence establishment of about 700 officers and men, two thirds were engaged in intercept or direction-finding activities and one third— including most of the 80 officers—in cryptanalysis and translation. Safford sized up the personnel of his three units this way: Pearl Harbor had some of the best officers, most of whom

had four or five years of radio intelligence experience; the crew at Corregidor, which in general had only two or three years' experience, was "young, enthusiastic, and capable"; Washington—responsible for both overall supervision and training—had some of the most experienced personnel, with more than ten years' experience, and many of the least: 90 per cent of the unit had less than a year's experience.

Under Safford in the three subsections most closely involved with cryptanalysis were Lieutenant Commanders George W. Welker of GX, the intercept and direction-finding subsection, Lee W. Parke of GY, the cryptanalytical subsection, and Kramer of GZ, the translation and dissemination subsection. GY attacked new systems and recovered new keys for solved systems, such as PURPLE. But while it made the initial breaks in code solutions, the detailed recovery of codegroups (which was primarily a linguistic problem as compared to the more mathematical cipher solutions) was left to GZ. Four officers in GY, assisted by chief petty officers, stood round-the-clock watches. Senior watch officer was Lieutenant (j.g.) George W. Lynn; the others were Lieutenants (j.g.) Brotherhood, Pering, and Allan A. Murray. GY had others on its staff, such as girl typists who also did the simple deciphering of some diplomatic messages after the watch officers and other cryptanalysts had found the keys.

Kramer was in an odd position. Though he worked in OP-20-GZ, he was formally attached to OP-16-F2—the Far Eastern Section of the Office of Naval Intelligence. This arrangement was intended in part to throw off the Japanese, who might have inferred some measure of success in codebreaking if a Japanese-language officer like Kramer were assigned to communications, in part to have an officer with a broad intelligence background distribute MAGIC so that he could answer the recipients' questions. Kramer, 38, who had studied in Japan from 1931 to 1934, had had two tours in O.N.I, proper before being assigned full time to GZ in June, 1940. An Annapolis graduate, chess fan, and rifle marksman, he lived in a world in which everything had one right way to be done. He chose his words with almost finicky exactness (one of his favorites was "precise"); he kept his pencil mustache trimmed to a hair; he filed his papers tidily; he often studied his MAGIC intercepts several times over before delivering them. Included in this philosophy was his duty. He performed it with great responsibility, intelligence, and dedication.

The first task of OP-20-G and of S.I.S. was to obtain intercepts. And in peacetime America that was not easy.

Section 605 of the Federal Communications Act of 1934, which prohibits wiretaps, also prohibits the interception of messages between foreign countries and the United States and territories. General Malin

Craig, Chief of Staff from 1937 to 1939, was acutely aware of this, and his attitude dampened efforts to intercept the Japanese diplomatic messages coming into America. But after General George C. Marshall succeeded to Craig's post, the exigencies of national defense relegated that problem in his mind to the status of a legalistic quibble. The crypt-analytic agencies pressed ahead in their intercept programs. The extreme secrecy in which they were cloaked helped them avoid detection. They concentrated on radio messages, since the cable companies, fully cognizant of the legal restrictions, in general refused to turn over any foreign communications to them. Consequently, 95 per cent of the intercepts were radio messages. The remainder was split between cable intercepts and photographs of messages on file at a few cooperative cable offices.

To pluck the messages from the airwaves, the Navy relied mainly on its listening posts at Bainbridge Island in Puget Sound; Winter Harbor, Maine; Cheltenham, Maryland; Heeia, Oahu; and Corregidor and to a lesser degree on stations at Guam; Imperial Beach, California; Amagansett, Long Island and Jupiter, Florida. Each station was assigned certain frequencies to cover. Bainbridge Island, which was called Station S, copied solid the schedule of Japanese government messages between Tokyo and San Francisco. Its two sound recorders guarded the radiotelephone band of that circuit; presumably it was equipped to unscramble the relatively simple sound inversion that then provided privacy from casual eavesdropping. Diplomatic messages were transmitted almost exclusively by commercial radio using roman letters. The naval radiograms, however, employed the special Morse code devised for kata kana, a syllabic script of Japanese. The Navy picked these up with operators trained in Japanese Morse and recorded them on a special typewriter that it had developed for the roman-letter equivalents of the kana characters. The Army's stations, called Monitor Posts, were: No. 1, Fort Hancock, New Jersey; No. 2, San Francisco; No. 3, Fort Sam Houston, San Antonio; No. 4, Panama; No. 5, Fort Shafter, Honolulu; No. 6, Fort Mills, Manila; No. 7, Fort Hunt, Virginia; No. 9, Rio de Janeiro.

At first both services airmailed messages from their intercept posts to Washington. But this proved too slow. The Pan-American Clipper, which carried Army intercepts from Hawaii to the mainland, departed only once a week on the average, and weather sometimes caused cancellations, forcing messages to be sent by ship. As late as the week before Pearl Harbor, two Army intercepts from Rio did not reach Washington for eleven days. Such delays compelled the Navy to install teletypewriter service in 1941 between Washington and its intercept stations in the continental U.S. The station would perforate a batch of intercepts onto a teleptype tape, connect with Washington through a teletypewriter exchange, and run the tape through mechanically at 60 words per minute, cutting toll charges to one third the cost of manually sending

each message individually. Outlying stations of both the Army and Navy picked out Japanese messages bearing certain indicators, enciphered the Japanese cryptograms in an American system, and radioed them to Washington. The reencipherment was to keep the Japanese from knowing of the extensive American cryptanalytic effort. Only the three top Japanese systems were involved in this expensive radio retransmission: PURPLE, RED (a machine system that antedated PURPLE, which had supplanted it at major embassies, but that was still in use for legations such as Vladivostok), and the J series of enciphered codes. The Army did not install a teletype for intercepts from its continental posts until the afternoon of December 6, 1941; the first messages (from San Francisco) were received in the early morning hours of December 7.

The intercept services missed little. Of the 227 messages pertaining to Japanese-American negotiations sent between Tokyo and Washington from March to December, 1941, all but four were picked up.

In Honolulu, where a large Japanese population produced nightmares of antlike espionage and potential sabotage, the 14th Naval District's intelligence officer, Captain Irving S. Mayfield, had long sought to obtain copies of the cablegrams of Consul General Nagao Kita. If Rochefort's unit could solve these, Mayfield figured, he might know better which Japanese to shadow and what information they sought.

His intuitions were sound. On March 27, 1941, not two weeks after Mayfield himself took up his duties, a young ensign of the Imperial Japanese Navy, 25-year-old Takeo Yoshikawa, who had steeped himself in information about the American Navy, arrived in Honolulu to serve as Japan's only military espionage agent covering Pearl Harbor. Under the cover-name "Tadasi Morimura," he was assigned to the consulate as a secretary. He promptly made himself obnoxious—and drew suspicion upon himself within the consulate staff—by coming to work late or not at all, getting drunk frequently, having women in his quarters overnight, and even insulting the consul himself on occasion. But he managed to tour the islands, and within a month was sending such messages as: "Warships observed at anchor on the llth [of May, 1941] in Pearl Harbor were as follows: Battleships, 11: *Colorado, West Virginia, California, Tennessee. . . ."* These were sent in the consulate's diplomatic systems, not in naval code.

But Mayfield's hopes of peering into these secret activities through the window of a broken code were stymied by the refusal of the cable offices to violate the statute against interception. So when David Sarnoff, president of the Radio Corporation of America, vacationed in Hawaii, Mayfield spoke to him. It was subsequently arranged that thenceforth R.C.A.'s Japanese consulate messages would be quietly given to the naval authorities. But the consulate rotated its business among the several cable companies in Honolulu, and R.C.A.'s turn was not due until

In Washington, however, intercepts overwhelmed GY and S.I.S. The tiny staff of cryptanalysts simply could not cope with all of them expeditiously. This difficulty was resolved in two ways.

One was to cut out duplication of effort. At first, both services solved all their Japanese diplomatic intercepts. But beginning more than a year before Pearl Harbor, messages originating in Tokyo on odd-numbered days of the month were handled by the Navy, those on even days, by the Army. Each began breaking the messages sent in from its own intercept stations until it reached the Tokyo date of origin; it would then retain them or send them over as the dates indicated. The cryptanalysts utilized the extra time to attack as-yet-unbroken systems and to clean up backlogs.

The other method was to concentrate on the important intercepts and let the others slide, at least until the important ones were completed. But how can a cryptanalyst tell which messages are important until he has solved them? He cannot, but he can assume that messages sent in the more secret systems are the more important. All dispatches cannot be transmitted in a single system because the huge volume of traffic would enable cryptanalysts to break it too quickly. Hence most nations set up a hierarchy of systems, reserving the top ones for their vital needs.

Japan was no exception. Though her Foreign Office employed an almost bewildering variety of different codes, resorting, from time to time, to the Yokohama Specie Bank's private code, a Chinese ideographic code list, and codes bearing kata kana names, such as TA, JI, or HEN, it relied in the main on four systems. American cryptanalysts ranked these on four levels according to the inherent difficulty of their solution and the messages that they generally carried. Intercepts were then solved in the order of this priority schedule.

Simplest of all, and hence the lowest in rank and last to be read (excluding plain language), was the LA code, so called from the indicator group LA that preceded its codetexts. LA did little more than put kata kana into roman letters for telegraphic transmission and to secure some abbreviation for cable economy. Thus the kana for *ki* was replaced by the code form CI, the kana for *to* by IF, the two-kana combination of *ka* + *n* by CE. Its two-letter codewords, all of either vowel-consonant or consonant-vowel form and including such as ZO for 4, were supplemented by a list of four-letter codewords, such as TUVE for *dollars,* SISA for *ryoji* ("consul"), and XYGY for *Yokohama.* A very typical LA message is serial 01250 from the Foreign Minister to Kita, dated December 4, which begins in translation: "The following has been authorized as the year-end bonus for employee typists of your office." This sort of code is generally called a

"passport code" because it usually serves for messages covering the administrative routine of a mission, such as issuance of passports and visas. LA was a particularly simple one to solve, partly because it had been in effect since 1925, partly because of the regularities in its construction. For example, all kana that ended in *e* had as code equivalents groups beginning with A *(ke* = AC, *se* = AD), and all that began with *k* had code equivalents beginning or ending with C. Identification of one kana would thus suggest the identification of others.

One rung up the cryptographic ladder was the system known to the Japanese as *Oite* and to American code-breakers as PA-K2. The PA part was a two- and four-letter code similar to the LA, though much more extensive and with codegroups disarranged. The K2 part was a transposition based on a keynumber. The letters from the PA encoding were written under this keynumber from right to left and then copied out in mixed order, taking first the letter under number 1, then the letter under number 2, until the row was completed. The process was repeated for successive rows.

For example, on December 4 Yoshikawa wired the Foreign Minister that "At 1 o'clock on the 4th a light cruiser of the *Honolulu* class hastily departed—Morimura." In romaji (the roman-letter version of the kata kana) this became *4th gogo 1 kei jun (honoruru) kata hyaku shutsu ko—morimura.* In PA, with the parentheses getting their own codegroups (OQ and UQ), it assumed this form: BYDH DOST JE YO IA OQ GU RA HY HY UQ VI LA YJ AY EC TY FI BANL, with FI indicating *use four-letter code.* (The code clerk made two errors. After encoding *kata* by VI, he encoded an extra *ta* into LA and an unnecessary *re* into TY.) This was then written under the keynumber from right to left, with an extra letter I as a null to complete the final five-letter group:

| 10 | 15 | 11 | 16 | 2 | 8 | 1 | 5 | 17 | 3 | 7 | 13 | 19 | 4 | 18 | 6 | 12 | 9 | 14 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| B | Y | D | H | D | O | S | T | J | E | Y | O | I | A | O | Q | G | U | R |
| A | H | Y | H | Y | U | Q | V | I | L | A | Y | J | A | Y | E | G | T | Y |
| | | | | F | | I | B | | A | N | | | L | | I | | | |

Transcribed line by line according to the numbers (s under 1 first, D under 2 second, etc.), prefixed with system indicator GIGIG and key indicator AUDOB, the message number, and the telegraphic abbreviation of *Sikuyu* ("urgent"), the message (with three more errors: the Y under 13 became the *J* in CJYHH, the F under 2 became the E in IYJIE, and the T under 9 became the i in AUIAY) became the one actually sent over Kita's name:

**GAIMUDAIJIN TOKIO**

**SIKYU 02500 GIGIG AUDOB SDEAT QYOUB DGORY HJOIQ YLAVE**

**AUIAY CJYHH IYJIE ALBIN**

**KITA**

PA-K2 did not pose much of a problem to experienced American cryptanalysts. ROchefort estimated that his unit could crack a PA-K2 message in from six hours to six days, with three days a good average. The transposition was vulnerable because each line was shuffled identically; the cryptanalyst could slice a cryptogram into groups of 15 or 17 or 19 and anagram these simultaneously until the predominant vowel-consonant alternation appeared on all lines; the underlying code could then be solved by assuming that the most frequent codegroups represented the most frequent kana *(i,* followed by *ma, shi, o,* etc.) and filling out the skeleton words that resulted. Since the system had remained in use for several years, this reconstruction had long been accomplished by the Washington agencies. Hence solution involved only unraveling any new transposition and, with luck, might take only a few hours. It could also take a few days. Primarily because of PA-K2's deferred position in the priority list, an average of two to four days elapsed between interception and translation.

The code clerk in Honolulu enveloped Yoshikawa's final messages in PA-K2 only because higher-level codes had been destroyed December 2 on orders from Tokyo. Normally, espionage reports of shipping movements and military activities, sent routinely by Japanese consuls from their posts all over the world, were framed on that next level of secrecy. Here prevailed a succession of codes called TSU by the Japanese and the J series by Americans. These were even more extensive and more thoroughly disarranged than PA, and they were transposed by a system of far greater complexity than the rather simple and vulnerable K2. Furthermore, the code and the transposition were changed at frequent intervals. Thus J17-K6 was replaced on March 1 by J18-K8, and that in turn by J19-K9 on August 1.

The transposition was the real stumbling block. Like the K2, it used a keynumber, but it differed in being copied off vertically instead of horizontally, and in having a pattern of holes in the transposition blocks. These holes were left blank when the code groups are inscribed into the block. For example, letting the alphabet from A to Y serve as the code message:

[CodeBreakers 020.jpg]

The letters were transcribed in columns in the order of the keynumbers, skipping over the blanks: BJMV EHKT NW CGORX AFILQU DPSY.

This would be sent in the usual five-letter groups.

The first step in solving a columnar transposition like this, but without blanks, is to cut the cryptogram into the approximately equal segments that the cryptanalyst believes represent the columns of the original block. The blanks vastly increase the difficulty of this essential first step because they vary the length of the column segments. The second step is to reconstruct the block by trying one segment next to the other until a codeword-like pattern appears. Here again the blanks, by introducing gaps in unknown places between the letters of the segments, greatly hinder the cryptanalyst.

The problems of solving such a system are illustrated by the fact that J18-K8 was not broken until more than a month after its introduction. The cryptanalysts had to make a fresh analysis for each pattern of blanks and each transposition key. The key changed daily, the blank-pattern three times a month. Hence J19-K9 solutions were frequently delayed. The key and pattern for November 18 were not recovered until December 3; those for November 28, not until December 7. On the other hand, solution was sometimes effected within a day or two. Success usually depended on the quantity of intercepts in a given key. About 10 or 15 per cent of J19-K9 keys were never solved.

This situation contrasts with that of PURPLE, the most secret Japanese system, in which all but 2 or 3 per cent of keys were recovered and in which most messages were solved within hours. Did the Japanese err in assessing the security of their systems? Yes and no. PURPLE was easier to keep up with once it was solved, but it was a much more difficult system to break in the first place than J19-K9. The solution of the PURPLE machine was, in fact, the greatest feat of cryptanalysis the world had yet known.

The cipher machine that Americans knew as PURPLE bore the resounding official Japanese title of 97-shiki O-bun In-ji-ki. This meant Alphabetical Typewriter '97, the '97 an abbreviation for the year 2597 of the Japanese calendar, which corresponds to 1937. The Japanese usually referred to it simply as "the machine" or as "J,"[1] the name given it by the Imperial Japanese Navy, which had adapted it from the German Enigma cipher machine and then had lent it to the Foreign Ministry, which, in turn, had further modified it. Its operating parts were housed in a drawer-sized box between two big black electrically operated Underwood typewriters, which were connected to it by 26 wires plugged into a row of sockets called a plugboard. To encipher a message, the cipher clerk would consult the thick YU GO book of machine keys, plug in the wire connections according to the key for the day, turn the four disks in the box so the numbers on their edges were those directed by the YU

GO, and type out the plaintext. His machine would record that plaintext while the other, getting the electric impulses after the coding box had twisted them through devious paths, would print out the cipher-text. Deciphering was the same, though the machine irritatingly printed the plaintext in the five-letter groups of the ciphertext input.

The Alphabetical Typewriter worked on roman letters, not kata kana. Hence it could encipher English as well as romaji—and also roman-letter codetexts, like those of the J codes. Since the machine could not encipher numerals or punctuation, the code clerk first transformed them into three-letter codewords, given in a small code list, and enciphered these. The receiving clerk would restore the punctuation, paragraphing, and so on, when typing up a finished copy of the decode.

The coding wheels and plugboards produced a cipher of great difficulty. The more a cipher deviates from the simple form in which one ciphertext letter invariably replaces the same plaintext letter, the harder it is to break. A cipher might replace a given plaintext letter by five different ciphertext letters in rotation, for example. But the Alphabetical Typewriter produced a substitution series hundreds of thousands of letters long. Its coding wheels, stepping a space—or two, or three, or four—after every letter or so, did not return to their original positions to re-create the same series of paths, and hence the same sequence of substitutes, until hundreds of thousands of letters had been enciphered. The task of the cryptanalysts consisted primarily of reconstructing the wiring and switches of the coding wheels—a task made more burdensome by the daily change of plugboard connections. Once this was done, the cryptanalyst still had to determine the starting position at the coding wheels for each day's messages. But this was a comparatively simple secondary job.

American cryptanalysts knew none of these details when the Japanese Foreign Office installed the Alphabetical Typewriter in its major embassies in the late 1930s. How, then, did they solve it? Where did they begin? How did they even know that a new machine was in service, since the Japanese government did not announce it?

The PURPLE machine supplanted the RED machine,[2] which American cryptanalysts had solved, and so probably their first clue to the new machine was the disconcerting discovery that they could no longer read the important Japanese messages. At the same time, they observed new indicators for the PURPLE system. Clues to the system's nature came from such characteristics of its ciphertext as the frequency of letters, the percentage of blanks (letters that did not appear in a given message), and the nature and number of repetitions. Perhaps the codebreakers also assumed that the new machine comprised essentially a more complicated and improved version of the one it replaced. In this they were right.

Their first essays at breaking into the cipher both accompanied and supplemented their attempts to determine the type of cipher. Their previous success with the RED machine and with the lesser systems had given them insight into the Japanese diplomatic forms of address, favorite phrases, and style (paragraphs were often numbered, for example). These provided the cryptanalysts with probable words—words likely to be in the plaintext— that would help in breaking the cipher. Opening and closing formulas, such as "I have the honor to inform Your Excellency" and "Re your telegram," constituted virtual cribs. Newspaper stories suggested the subject matter of intercepts. The State Department sometimes made public the full texts of diplomatic notes from Japan to the American government, in effect handing the cryptanalysts the plaintext (or its translation) of an entire dispatch. (State reportedly did not pass the texts of confidential notes to the cryptanalysts, though this would have helped them considerably and was done by other foreign ministries.) Japan's Foreign Office often had to circulate the same text to several embassies, not all of which had a PURPLE machine, and a code clerk might have inadvertently encoded some cables in PURPLE, some in other systems— which the cryptanalysts could read. A comparison of times of dispatch and length, and *voilá!*—another crib to a cryptogram. Errors were, as always, a fruitful source of clues. As late as November, 1941, the Manila legation repeated a telegram "because of a mistake on the plugboard." How much more common must errors have been when the code clerks were just learning to handle the machine! The sending of the identical text in two different keys produces "isomorphic" cryptograms that yield exceedingly valuable information on the composition of the cipher.

The cryptanalysts of S.I.S. and OP-20-G, then, matched these assumed plaintexts to their ciphertexts and looked for regularities from which they could derive a pattern of encipherment. This kind of work, particularly in the early stages of a difficult cryptanalysis, is perhaps the most excruciating, exasperating, agonizing mental process known to man. Hour after hour, day after day, sometimes month after month, the cryptanalyst tortures his brain to find some relationship between the letters that hangs together, does not dead-end in self-contradiction, and leads to additional valid results.

The codebreakers attacking the new Japanese mechanism went just so far—and for months could not push on further. As William Friedman recalled, "When the PURPLE system was first introduced it presented an extremely difficult problem on which the Chief Signal Officer [Mauborgne] asked us to direct our best efforts. After work by my associates when we were making very slow progress, the Chief Signal Officer asked me personally to take a hand. I had been engaged largely in administrative duties up to that time, so at his request I dropped everything else that I could and began to work with the group."

Lighting his way with some of the methods that he himself had developed, he led the cryptanalysts through the murky PURPLE shadowland. He assigned teams to test various hypotheses. Some prospected fruitlessly, their only result a demonstration that success lay in another direction. Others found bits and pieces that seemed to make sense. (OP-20-G cooperated in this work, with Harry L. Clark making especially valuable contributions, but S.I.S. did most of it.) Friedman and the other codebreakers began to segregate the ciphertext letters into cycles representing the rotation of the coding wheels—gingerly at first, then faster and faster as the evidence accumulated. The polyalphabetic class of ciphers, to which PURPLE belonged, is based ultimately upon an alphabet table, usually 26 letters by 26. To reconstruct the PURPLE tables, the cryptanalysts employed both direct and indirect symmetry of position— names only slightly less forbidden than the methods they denote. Errors, caused perhaps by garbled interceptions or simple mistakes in the cryptanalysis, jarred these delicate analyses and delayed the work. But slowly it progressed. A cryptanalyst, brooding sphinxlike over the cross-ruled paper on his desk, would glimpse the skeleton of a pattern in a few scattered letters; he tried fitting a fragment from another recovery into it; he tested the new values that resulted and found that they produced acceptable plaintext; he incorporated his essay into the over-all solution and pressed on. Experts in Japanese filled in missing letters; mathematicians tied in one cycle with another and both to the tables. Every weapon of cryptanalytic science—which in the stratospheric realm of this solution drew heavily upon mathematics, using group theory, congruences, Poisson distributions—was thrown into the fray.

Eventually the solution reached the point where the cryptanalysts had a pretty good pencil-and-paper analog of the PURPLE machine. S.I.S. then constructed a mechanism that would do automatically what the cryptanalysts could do manually with their tables and cycles. They assembled it out of ordinary hardware and easily available pieces of communication equipment, such as the selector switches used for telephones. It was hardly a beautiful piece of machinery, and when not running just right it spewed sparks and made loud whirring noises. Though the Americans never saw the 97-shiki O-bun In-ji-ki, their contraption bore a surprising physical resemblance to it, and of course exactly duplicated it cryptographically.

S.I.S. handed in its first complete PURPLE solution in August of 1940, after 18 or 20 months of the most intensive analysis. In looking back on the effort that culminated in this, the outstanding cryptanalytic success in the whole history of secret writing up to its time, Friedman would say generously:

> Naturally this was a collaborative, cooperative effort on the part

> of all the people concerned. No one person is responsible for the solution, nor is there any single person to whom the major share of credit should go. As I say, it was a team, and it was only by very closely coordinated teamwork that we were able to solve it, which we did. It represents an achievement of the Army cryptanalytic bureau that, so far as I know, has not been duplicated elsewhere, because we definitely know that the British cryptanalytic service and the German cryptanalytic service were baffled in their attempts and they never did solve it.

Friedman, was, despite his partial disclaimer, the captain of that team. The solution had taken a terrific toll. The restless turning of the mind tormented by a puzzle, the preoccupation at meals, the insomnia, the sudden wakening at midnight, the pressure to succeed because failure could have national consequences, the despair of the long weeks when the problem seemed insoluble, the repeated dashings of uplifted hopes, the mental shocks, the tension and the frustration and the urgency and the secrecy all converged and hammered furiously upon his skull. He collapsed in December. After three and a half months in Walter Reed General Hospital recovering from the nervous breakdown, he returned to S.I.S. on shortened hours, working at first in the more relaxed area of cryptosecurity. By the time of Pearl Harbor he was again able to do some cryptanalysis, this time of German systems.

OP-20-G contributed importantly to the ease and speed of daily PURPLE solutions when 27-year-old Lieutenant (j.g.) Francis A. Raven discovered the key to the keys. After a number of PURPLE messages has been solved, Raven observed that the daily keys within each of the three ten-day periods of a month appeared to be related. He soon found that the Japanese simply shuffled the first day's key to form the keys for the next nine days, and that the nine shuffling patterns were the same in all the ten-day periods. Raven's discovery enabled the cryptanalysts to predict the keys for nine out of ten days. The cryptanalysts still had to solve for the first day's key by straightforward analysis, but this task and its delays were eliminated for the rest of the period. Furthermore, knowledge of the shuffles enabled the codebreakers to read all the traffic of a period even though they could solve only one of the daily keys.

This fine piece of work, on the shoulders of the tremendous initial Friedman-S.I.S. effort, resulted in the paradoxical situation of Americans reading the most difficult Japanese diplomatic system more quickly and easily than some lower-grade systems. They also became very facile in reading two-step systems in which PURPLE superenciphered an already coded message. The Japanese did this from time to time to provide extra security, usually with the CA code, the personal code of an ambassador or head of mission. A year after S.I.S. handed in its first PURPLE solution, the

cryptanalysts solved a message enciphered in "the highest type of secret classification used by the Japanese Foreign Office." The message was first enciphered in CA; this was then juggled according to the K9 transposition (normally used with the J19 code), and the transposed codetext was then enciphered on the PURPLE machine. The solution, which on the basis of the number of combinations involved might have been expected to take geologic eons, was completed in just four days.

The intercepts ordinarily needed to be translated, and translation was the bottleneck of the MAGIC production line. Interpreters of Japanese were even scarcer than expert cryptanalysts. Security precluded employing Nisei or any but the most trustworthy Americans. Through prodigious efforts in 1941 the Navy doubled its GZ translation staff —to six. These included three whom Kramer called "the most highly skilled Occidentals in the Japanese language in the world."

But ability in standard Japanese alone did not suffice. Each translator had to have at least a year's experience in telegraphic Japanese as well before he could be trusted to come through with the correct interpretation of a dispatch. This is because telegraphic Japanese is virtually a language within a language, and, as McCollum, himself a Japanese-language officer, explained, "the so-called translator in this type of stuff almost has to be a cryptographer himself. You understand that these things come out in the form of syllables, and it is how you group your syllables that you make your words. There is no punctuation.

"Now, without the Chinese ideograph to read from, it is most difficult to group these things together. That is, any two sounds grouped together to make a word may mean a variety of things. For instance, 'ba' may mean horses or fields, old women, or my hand, all depending on the ideographs with which it is written. On the so-called translator is forced the job of taking unrelated syllables and grouping them into what looks to him to be intelligible words, substituting then such of the Chinese ideographs necessary to pin it down, and then going ahead with the translation, which is a much more difficult job than simple translation."

Hence the situation of Mrs. Dorothy Edgers. She had lived for thirty years in Japan and had a diploma from a Japanese school to teach Japanese to Japanese students up to high-school level. Yet, because she had only two weeks' experience in GZ at the time of Pearl Harbor, Kramer considered her "not a reliable translator" in this field. And on the important messages, only reliable translators could be used. To unclog this bottleneck, messages in the minor systems were given only a partial translation. If a translator saw that they dealt with administrative trivia, they were frequently not formally translated at all.

With manifold streamlinings like that, with enlarged staffs, with the

fluidity gained by experience, OP-20-G and S.I.S. gradually increased the speed and quality of their output. In 1939, the agencies had often required three weeks to funnel a message from interceptor to recipient. In the latter part of 1941 the process sometimes took as little as four hours. Occasionally an agency broke down a late intercept that bore on a point of Japanese-American negotiations and rushed it to the Secretary of State an hour before he was to meet with the Japanese ambassadors. Volume attained overwhelming proportions. By the fall of 1941, 50 to 75 messages a day sluiced out of the two agencies, and at least once the quantity swelled to 130. Some of these messages ran to 15 typewritten pages.

The top-echelon recipients of MAGIC clearly could not afford the time to read all this traffic. Much of it was of secondary importance anyway. Kramer and Colonel Rufus S. Bratton, army G-2 Far Eastern Section chief, winnowed the wheat from this chaff. Reading the entire output, they chose an average of 25 messages a day for distribution. At first Kramer supplemented his translations with gists for recipients too busy to read every word of the actual intercepts, starring the important ones, but he abandoned these in mid-November under the pressure of getting out the basic material. Bratton, who had been delivering summaries of MAGIC in the form of Intelligence Bulletins, began on August 5 to distribute MAGIC verbatim at Marshall's orders. This, however, had the effect of increasing the volume. Marshall complained that to absorb every word of it he would have had to "retire as Chief of Staff and read every day." To save the recipients' time, Bratton checked the important messages on a list in the folder with a red pencil; Kramer slid paper clips onto them. The recipients always read the flagged messages; the others they did not always study, but they did skim them.

Distribution was usually made twice a day. Intercepts that had come in overnight went out in the morning, those processed during the day went out at the end of the afternoon. Especially important messages were delivered at once, often to the recipients' homes if late in the evening. Each agency sent its MAGIC copies on to the other with exemplary promptitude, despite a natural competition between them.

As Bratton put it: "I was further urged on by the fact that if the Chief of Naval Operations ever got one of these things before General Marshall did and called him up to discuss it on the telephone with him, and the General hadn't gotten his copy, we all caught hell." (Marshall demurred: "I don't think I gave anybody hell much.")

Delivery to the White House and the State Department incurred difficulties. Under an agreement of January 23, the Army and Navy at first alternated in servicing the two. The Army, however, discontinued its deliveries to the White House after its turn in May, partly because a military aide made a security bungle, partly because it felt that these

diplomatic matters should go to the President through the State Department. The Navy continued its deliveries through the President's naval aide, Captain John R. Beardall, though once in the summer Kramer himself carried a particularly "hot" message—probably dealing with negotiations the next day—to Roosevelt. Near the end of September, a month originally scheduled for Army delivery, during which nothing was delivered to the White House, the President said he wanted to see the intercept information. In October naval intelligence sent him memoranda based on MAGIC, but on Friday, November 7, Roosevelt said he wanted to see MAGIC itself. Beardall told him that it was an Army month. The President replied that he knew that and that he was either seeing MAGIC or getting information on it from Hull, but that he still wanted to see the original intercepts. He feared that condensing them would distort their meaning. On Monday, a conference agreed that the Navy would furnish the White House with MAGIC and the Army the State Department. At 4:15 p.m., Wednesday, November 12, Kramer made the first distribution to the White House under this system.

Thus, by the fall of 1941, MAGIC was being demanded at the topmost level of government. It had become a regular and vital factor in the formation of American policy. Hull, who looked upon MAGIC "as I would a witness who is giving evidence against his own side of the case," was "at all times intensely interested in the contents of the intercepts." The chief of Army intelligence regarded MAGIC as the most reliable and authentic information that the War Department was receiving on Japanese intentions and activities. The Navy war plans chief thought that MAGIC, which was largely diplomatic at this time, affected his estimates by about 15 per cent. The high officials not only read MAGIC avidly and discussed it at their conferences, they acted upon it. Thus the decision to set up the command of United States Army Forces, Far East, which was headed by General MacArthur, stemmed in part from intercepts early in 1941 showing that Germany was pressuring Japan to attack Britain in Asia in the hope of involving the United State in the war; on the basis of this information, the command was created in July to deter Japan by enhancing American prestige in the Western Pacific—and it is a fact that Japan did not then comply with Germany's wishes.

The intricate mechanism of the American cryptanalytic effort pumped MAGIC to its eager recipients smoothly, speedily, and lavishly. Messages flew back and forth along the monitor channels as if along nerve cells. Intercepts poured into Washington with less and less of a time lag. S.I.S. and GY grew increasingly adept at solution; the translators picked out the important messages ever more surely. Bratton and Kramer hustled from place to place with their locked briefcases. MAGIC gushed forth in profusion. So effectively did the cryptanalytic agencies perform that Marshall could say of this "priceless asset," this most complete and up-to-the-minute intelligence that any nation had ever had concerning a

probable enemy, this necromantic gift of the gods of which one could apparently never have enough, that "There was too much of it."

## 2. One Day of Magic: II

IN October the cabinet of Prince Konoye fell, and the Emperor summoned General Hideki Tojo to form a new government. One of the first acts of the new Foreign Minister, Shigenori Togo, was to call in the chief of the cable section. Togo, remembering a book that Herbert O. Yardley had written disclosing his 1920 solution of Japanese diplomatic codes, asked the cable chief, Kazuji Kameyama, whether their current diplomatic communications were secure. Kameyama reassured him. "This time," he said, "it's all right."

With the assumption of total power by the militarists under Tojo, the last real hopes for peace died. Almost at once, events began to slide toward war. On November 4, Tokyo sent to her ambassadors at Washington the text of her proposal B, which Togo described as "absolutely final." The ambassadors held it while they pursued other avenues, even though Tokyo, on November 5, told them that "Because of various circumstances, it is absolutely necessary that all arrangements for the signing of this agreement be completed by the 25th of this month."

That same day, Yamamoto promulgated Combined Fleet Top Secret Order Number 1, the plan for the Pearl Harbor attack. Two days later, he set December 8 (Tokyo time) as Y-day and named Vice Admiral Chuichi Nagumo as Commander, First Air Fleet—the Pearl Harbor strike force. In the days that followed, the 32 ships that were to compose the force slipped, one by one, out to sea and vanished. Far from any observation, they headed north to rendezvous in a bay of barren Etoforu Island, one of the chill, desolate Kuriles north of the four main islands of Japan. Behind them the ships left their regular wireless operators to carry on an apparently routine radio traffic in their own "fists," or sending touch, which is as distinctive as handwriting.

As the force was gathering, the Foreign Office, which knew only that the situation was tense and was never told in advance of the time, place, or nature of the planned attack, prepared on open-code arrangement as an emergency means of notification. Tokyo sent Circular 2353 to Washington on November 19:

> Regarding the broadcast of a special message in an emergency.
>
> In case of emergency (danger of cutting off our diplomatic

relations), and the cutting off of international communications, the following warning will be added in the middle of the daily Japanese language short-wave news broadcast:

1) In case of Japan-U.S. relations in danger: HIGASHI NO KAZE AME ("east wind rain")

2) Japan-U.S.S.R. relations: KITA NO KAZE KU-MORI ("north wind cloudy")

3) Japan-British relations: NISHE NO KAZE HARE ("west wind clear")

This signal will be given in the middle and at the end as a weather forecast and each sentence will be repeated twice. When this is heard please destroy all code papers, etc. This is as yet to be a completely secret arrangement.

Forward as urgent intelligence.

This open code related the winds to the compass points in which the named countries stood in regard to Japan: the U.S. to the east, Russia to the north, England to the west. Tokyo also set up an almost similar code for use in the general intelligence (not news) broadcasts.

As the secret messages establishing these open codes whistled through the air, Navy intercept Station S at Bainbridge Island heard and nabbed them. The station teletyped them to GY, which identified them as J19 and began cryptanalysis.

Many of the ships of the Pearl Harbor strike force had by then gathered in bleak Tankan Bay, where the only signs of human presence were a small concrete pier, a wireless shack, and three fishermen's huts. Snow covered the surrounding hills. In the gray twilight of November 21, the great carrier *Zuikaku* glided into the remote harbor to complete the roster. The force swung at anchor, awaiting the order to sortie.

A few hours later, on November 20 (Washington time), the Japanese ambassador to the United States, Admiral Kichisaburo Nomura, and his newly arrived associate, Saburo Kurusu, presented Japan's ultimatum to Hull. It would have required the United States to reverse its foreign policy, acquiesce in further Japanese conquests, supply Japan with as much oil as she required for them, abandon China, and in effect surrender to international immorality. While Hull began drafting a reply, Tokyo cabled its ambassadors in message 812 that "There are reasons beyond your ability to guess why we wanted to settle Japanese-American relations by the 25th, but if within the next three or four days you can finish your conversations with the Americans; if the signing can be completed by the 29th (let me write it out for you—twenty-ninth); if the

pertinent notes can be exchanged; if we can get an understanding with Great Britain and the Netherlands; and in short if everything can be finished, we have decided to wait until that date. This time we mean it, the deadline absolutely cannot be changed. After that things are automatically going to happen." Two days later, Togo wirelessed: "The time limit set in my message No. 812 is in Tokyo time." The calendar had become a clock, and the clock had begun to tick.

On November 25, Yamamoto ordered the Pearl Harbor strike force to sortie next day. At 6 a.m. on November 26, the 32 ships of the force—six carriers, two battleships, and a flock of destroyers and support vessels—weighed anchor and sliced across the wrinkled surface of Tankan Bay. They steamed slightly south of east, heading into the "vacant sea"—the wintry North Pacific, whose wastes were undefiled by merchant tracks and whose empty vastness would swallow up the force. They had been ordered to return if detected before December 6 (Tokyo time); if discovered on December 7, Nagumo would decide whether or not to attack. Strict radio silence was enjoined. Aboard the battleship *Hiei,* Commander Kazuyoshi Kochi, a communications officer for the force, removed an essential part of his transmitter and put it in a wooden box, which he used as a pillow. The force drove eastward through fog, gale winds, and high seas. No one saw them.

Meanwhile, Hull, after a frantic week of drafting, consultations, and redraftings, had completed the American reply to Japan's proposal. It called upon Japan to withdraw all forces from China and Indochina and in return promised to unfreeze Japanese funds and resume trade. Nothing was said about oil. On November 26, the day that he handed it to Nomura, Tokyo circularized its major embassies with an open code. While the winds code envisioned abolition of all communication with the embassies, this new code—called the INGO DENPO ("hidden word") code — was intended for a less critical situation. It seems to have been arranged at the request of the consul in Singapore in case code but not plain language telegrams were prohibited. It set up such equivalences as ARIMURA = *code communications prohibited;* HATTORI = *relations between Japan and (name of country) are not in accordance with expectation;*[3] KODAMA = *Japan;* KUBOTA = *U.S.S.R.;* MINAMI =*U.S.A.;* and so on. "In order to distinguish these cables from others," Tokyo said, "the English word STOP will be added at the end as an indicator. (The Japanese word OWARI [end] will not be used.)"

The next day, November 28, the Navy cracked the transposition for the J19 message of nine days earlier and learned of the winds code arrangement. The cryptanalytic agencies saw at once that this arrangement, which dispensed with the entire routine of coding, cabling, delivery, and decoding, could give several hours' advance warning of

Japan's intentions. They erupted into activity to try to intercept it. This wrenched facilities away from the commercial (for Japanese diplomatic), naval, and radiotelephone circuits with which the agencies were familiar and put them on voice newscasts.

The Army asked the Federal Communications Commission to listen for the winds code execute. Army stations at Hawaii and San Francisco tuned to the newscasts, as did Navy stations at Corregidor, Hawaii, and Bainbridge Island, and four or five along the Atlantic seaboard. Rochefort placed his four best language officers—Lieutenants Forrest R. Biard, J. R. Bromley, Allyn Cole, Jr., and G. M. Slonim—on a 24-hour watch on frequencies suggested by Washington and on others that his unit had found. The Dutch in Java and the British in Singapore listened. In Washington, Kramer made up some 3x5 cards for distribution to MAGIC recipients. They bore only the portentous phrases, "East Wind Rain: United States. North Wind Cloudy: Russia. West Wind Clear: England."

Soon plain-language intercepts were swamping GZ. Bainbridge ran up bills of $60 a day to send them in. Kramer and the other translators, already burdened, now had also to scan 100 feet of teletype paper a day for the execute; previously only three to five feet per week of plain language material had come in. The long strips were thrown into the wastebasket and burned after checking. Several times the GY watch officers telephoned Kramer at his home at night to ask him to come to the office and check a possible execute. It always proved false.

Meanwhile, other signs of increasing tension were not lacking. On the 29th, Baron Oshima in Berlin reported that the German Foreign Minister, Joachim von Ribbentrop, had told him, "Should Japan become engaged in a war against the United States, Germany, of course, would join the war immediately." Next day, Tokyo replied, "Say very secretly to them that there is extreme danger that war may suddenly break out between the Anglo-Saxon nations and Japan through some clash of arms and add that the time of the breaking out of this war may come quicker than anyone dreams." Both these messages were translated on December 1, and Roosevelt considered the latter so important that he asked for a copy of it to keep. Kramer, after paraphrasing it for security's sake, gave him one.

At Pearl Harbor, Rochefort had just been presented with an unpleasant confirmation of that tautening situation. The Japanese fleet reassigned its 20,000 radio call-signs at midnight, December 1—only 30 days after the previous change. It was the first time in Rochefort's experience that a switch had occurred so soon after a previous one.

The one on November 1 had been expected; it had followed by the usual six months the regular spring call-sign shift. With the facility born

of long experience, Rochefort's Combat Intelligence Unit identified in fairly rapid order the senders and receivers of a large percentage of the traffic. The unit observed the rising volume and southward routing of messages on the 200 radio circuits of the Japanese Navy. This fitted in almost perfectly with the widely known Japanese buildup for what the world thought was a strike at Siam or Singapore. By the third week in November, the unit had sensed the formation of a Third Fleet task force and its imminent departure in the direction of those areas. Aircraft carriers were not addressed during this buildup, nor did they transmit. To Rochefort, the situation shaped up like those of February and July, when Japanese fleet units moved south to support the takeover in French Indochina while the carriers remained in home waters as a reserve. They were there, he felt, to protect the exposed flank of the Japanese forces from the American fleet, which, from its bases at Cavite and Pearl, could sever the supply lines of the aggressor.

Rochefort's view was shared by fleet intelligence officer Layton. He knew that the two main carrier divisions had not appeared in the traffic for at least two weeks, and maybe three. He suspected their presence in home waters, but since he lacked positive indications of it, he omitted his presumptions from a report on the Japanese fleet that he submitted to Kimmel on December 1. Whereupon, Layton recalled:

> Admiral Kimmel said, "What! You don't know where Carrier Division 1 and Carrier Division 2 are!"
>
> I replied, "No sir, I do not. I think they are in home waters, but I do not know where they are. The rest of these units, I feel pretty confident of their location." Then Admiral Kimmel looked at me, as sometimes he would, with somewhat a stern countenance and yet partially with a twinkle in his eye, and said:
>
> "Do you mean to say that they could be rounding Diamond Head and you wouldn't know it?" or words to that effect. My reply was that "I hope they would be sighted before now," or words to that effect.

On the same day that Layton gave his report to Kimmel, the Office of Naval Intelligence produced a memorandum of "Japanese Fleet Locations" that Layton, when he saw it, considered as "dotting the i's and crossing the t's" of his own estimates. It placed *Akagi* and *Kaga* (Carrier Division 1), and *Koryu* and *Kasuga* in southern Kyushu waters, and *Soryu* and *Hiryu* (Carrier Division 2) and *Zuikaku, Shokaku, Hosho,* and *Ryujo* at the great naval base of Kure. All this was just a more precise way of saying "home waters."

These estimates were based on the November observations. The call-

sign change of December 1 obliterated the intricate communication networks that the radio intelligence units had so painstakingly built up and forced them to begin anew. The Japanese bedeviled them with new communication-security measures. Dispatches were sent “on the umbrella"—broadcast to the fleet at large and copied by all ships. This sort of blanket coverage made identification difficult. Multiple addresses were used. They sent dummy traffic, which, however, did not confuse the listeners. Just before the change, the communicators passed many old messages. Rochefort's unit spotted them, and guessed that they were attempts either to pad the volume or to get through to the addressee before the change caused routing difficulties.

On December 2, after only two days of analyzing the new calls, Rochefort's unit stated in its Communications Intelligence Summary: "Carriers—Almost a complete blank of information of the Carriers today. Lack of identifications has somewhat promoted this lack of information. However, since over two hundred service calls have been partially identified since the change on the first of December and not one carrier call has been recovered, it is evident that carrier traffic is at a low ebb." In the next day's summary appeared the last mention of carriers before December 7, and it was rather negative: "No information on submarines or carriers."

Other messages, however, clearly indicated the drive to the south, which Japan made no attempt to conceal. Twice before, Rochefort, Fabian, Layton, and O.N.I, had seen exactly the same conditions, and twice before their reasoning that the carriers were being held in empire waters had been proved right. Now, they thought, they were seeing it happen again. Temporarily oblivious to the possibility of a surprise attack on Pearl Harbor, they watched the forces moving against Malaya as hypnotically as a conjuror's audience stares at the empty right hand while the left is pulling the ace out of a sleeve.

American preconceptions were reinforced by two PURPLE messages of December 1, which the Navy read that same day. In the first, Tokyo directed Washington: "When you are faced with the necessity of destroying codes, get in touch with the naval attache's office there and make use of chemicals they have on hand for this purpose. The ATTACHÉ should have been advised by the Navy Ministry regarding this." Five days earlier, the cryptanalysts had read Tokyo's detailed instructions on how to destroy the PURPLE machine in an emergency. These two code-destruction messages appeared to be just precautionary measures in a tense situation, and this impression was strengthened by the second message of December 1. It seemed to virtually announce a Japanese invasion of British and Dutch possessions and to relegate conflict with the United States to a subsequent date: "The four offices in London,

Hong-kong, Singapore and Manila have been instructed to abandon the use of the code machines and to dispose of them. The machine in Batavia has been returned to Japan. Regardless of the contents of my circular message #2447 [which MAGIC did not have], the U.S. (office) retains the machines and the machine codes." American officials breathed easier. The messages appeared to give the United States a bit more of what it needed most—time, time to build up its pitifully weak Army and Navy.

While the world gazed with tunnel vision toward Southeast Asia, and American radio intelligence envisioned the Japanese carriers in home waters, six of them—*Akagi, Kaga, Hiryu, Soryu, Shokaku,* and *Zuikaku*—were in fact butting eastward through the high winds and waves of the vacant sea. Late in the afternoon of December 2, Tokyo time, the force picked up, apparently on a blanket broadcast, an electrifying open-code message intended for it: NIITAKA-YAMA NOBORE ("Climb Mount Niitaka"). It informed the strike force that the decision for war had been made and directed it to *proceed with attack.* Niitaka-yama, also known as Mount Morrison, is a peak on Formosa whose 12,956-foot elevation made it the highest point of what was then the Japanese empire. The symbolism could not have been lost on the officers. The force refueled from its tankers.

Earlier that day, the Japanese consulate in Honolulu had received Circular #*2445 in* J19, relayed by Washington from Tokyo:

> Take great pains that this does not leak out. You are to take the following measures immediately:
>
> 1. With the exception of one copy each of the O [PA-K2] and the L [LA] codes, you are to burn all telegraph codes (this includes the codebooks for communication between the three departments [HATO] and those for use by the Navy).
>
> 2. As soon as you have completed this operation, wire the one word HARUNA.
>
> 3. Burn all secret records of incoming and outgoing telegrams.
>
> 4. Taking care not to arouse outside suspicion, dispose of all secret documents in the same way.
>
> Since these measures are in preparation for an emergency, keep this within your consulate and carry out your duties with calmness and care.

The codes were duly burned, including the TSU, or J19, in which the circular was transmitted. That evening Kita sent HARUNA. Henceforth the consulate code secretary, Samon Tsukikawa, would have to transmit the spy messages of Yoshikawa, alias Morimura, in the simpler PA-K2. The first such message arranged four signaling systems by which a spy might report on the condition of the ships in Pearl Harbor. The arrangement had been submitted to Yoshikawa by an Axis spy in Hawaii, Bernhard Julius Otto Kühn. Nazi Propaganda Minister Josef Goebbels had transferred him to the islands in 1935 after a contretemps with Kühn's daughter Ruth, who had become Goebbels' mistress when she was 16. In his signaling system, Kühn stipulated that numbers from 1 to 8 would mean such things as *A number of carriers preparing to sortie* (which was 2) and *Several carriers departed between 4th and 6th* (which was 7). Then he arranged that bonfires, house lights shown at certain times and places, or want ads broadcast over radio station KGMG would mean certain numbers. For example, 7 would be represented by two lights shown in the window of a house on Lanikai Beach between 2 and 3 a.m., or by two sheets between 10 and 11 a.m., by lights in the attic window of a house in Kalama between 11 and 12 p.m., or by a want ad offering a complete chicken farm for sale and listing P.O. Box 1476. If all these failed, a bonfire on a certain peak of Maui Island between 8 and 9 p.m. would indicate 7. The purpose of the system was to eliminate dangerous personal contacts between Kühn and the Japanese. Kühn tested it on December 2, found that it worked, and passed it to Yoshikawa. He had it encoded (in PA-K2) and sent to Tokyo in two long parts on December 3.

It was now the third day of the month in which the Japanese consulate gave its cable business to R.C.A. Following Sarnoff's instructions, George Street, district manager of the firm, had had the Japanese consulate messages copied on a blank sheet of paper with no identification of the sender or addressee. About 10 or 11 a.m., December 3, Mayfield called at the branch office and Street slipped him a blank envelope containing the messages. As soon as Mayfield returned to the District Intelligence Office, he had a messenger bring them down to Rochefort.

In Washington that Wednesday, the Signal Intelligence Service solved a PURPLE message from Tokyo—and the readers of MAGIC, who only two days earlier had been lulled by the supposition that Japan might temporarily spare the United States, were stunned by the realization that the arrow of war might be loosed momentarily. For the message ordered the Washington embassy to "burn all [codes] but those now used with the machine and one copy each of o code [PA-K2] and abbreviating code [LA]. . . . Stop at once using one code machine unit and destroy it

completely . . . wire . . . HARUNA." Under Secretary of State Welles saw it and felt that "the chances had diminished from one in a thousand to one in a million that war could then be avoided." When the President's naval aide, Beardall, brought the message to Roosevelt, he said in substance, "Mr. President, this is a very significant dispatch." After the Chief Executive had read it carefully, he asked Beardall, "When do you think it will happen?"—referring to the outbreak of war. "Most any time," replied the naval aide, who thought that the moment was getting very close.

At the Japanese embassy at 2514 Massachusetts Avenue, the code clerks were executing these destruction orders. The code room stood at the southeast corner of the embassy, with windows overlooking the embassy parking lot and another legation next door. Half a dozen desks clustered in the middle of the room. Two cipher machines waited on desks against the west wall and a third, broken, rested in the walk-in safe. In utter disregard of the regulations promulgated for the security of communications, the embassy had hired an elderly Negro janitor named Robert to dust and clean the code room and its supersecret furnishings each day. The code clerks did make some obeisance to the security regulations by not allowing him in the room unless some Japanese were in it. But the situation was, to say the least, ironical. While the Japanese Foreign Office was exercising almost superhuman security precautions and American cryptanalysts were suffering nervous breakdowns to solve the PURPLE machine, an American citizen was running his duster over tables on which stood the intricate machines that were the vortex of this silent struggle.

But just as the Japanese seemed not to have given serious thought to the possibility of Robert's being a spy, so the Americans seemed to have given no serious thought to the possibility that a spy might have been insinuated into the Japanese embassy to ease their cryptanalytic burden. Of course, even if they had thought about it, they might have rejected the idea, for discovery of the spy would have meant an automatic change of codes. The danger of this was much less if the systems were read through cryptanalysis.

The paper codes of the Japanese consisted of folders whose four or six pages could be opened into a single long sheet. Embassy Counselor Sadao Iguchi, who was in charge of the code room, directed telegraph officer Masana Horiuchi and code clerks Takeshi Kajiwara, Hiroshi Hori, Juichi Yoshida, Tsukao Kawabata and Kenichiro Kondo in the burning of the paper codes. Demolition of the code machine was more complicated, and followed the guidelines transmitted recently by the Foreign Office. The machines were dismantled with a screwdriver, hammered into unrecognizability, and then dissolved in acid from the naval attache's office to destroy them thoroughly. Some of these operations were carried out in the gardens of the embassy; so when Bratton, who had read the

code-destruction intelligence, sent an officer to the embassy to check, he obtained immediate confirmation.

Now the American officials realized the ominous meaning of the HARUNA messages that had been intercepted as they were sent from New York, New Orleans, and Havana and that had been received just that day in S.I.S. The Army and Navy high command universally regarded the destruction of codes as virtual certainty that war would break out within the next few days. As Stark's deputy put it: "If you rupture diplomatic negotiations you do not necessarily have to burn your codes. The diplomats go home, and they can pack up their codes with their dolls and take them home. Also, when you rupture diplomatic negotiations you do not rupture consular relations. The consuls stay on. Now, in this particular set of dispatches they not only told their diplomats in Washington and London to burn their codes, but they told their consuls in Manila, in Hong Kong, Singapore, and Batavia to burn their codes and that did not mean a rupture of diplomatic relations; it meant war."

A few hours after the code-destruction MAGIC reached Stark, he dispatched the electrifying news to Kimmel and Hart:

> Highly reliable information has been received that categoric and urgent instructions were sent yesterday to Japanese diplomatic and consular posts at Hongkong X Singapore X Batavia X Manila X Washington and London to destroy most of their codes and ciphers at once and to burn all other important confidential and secret documents X

He followed this five minutes later with another message:

> Circular twenty four forty four from Tokyo one December ordered London X Hongkong X Singapore and Manila to destroy PURPLE machine XX Batavia machine already sent to Tokyo XX December second Washington also directed destroy PURPLE X all but one copy of other systems X and all secret documents XX British Admiralty London today reports embassy London has complied

In Washington urgency drove out all thoughts of security. The strict injunction against ever mentioning MAGIC was completely overlooked. When Kimmel got the message, he asked Layton what "PURPLE" was. So tight had security been that neither of them knew. They checked with Lieutenant Herbert M. Coleman, the fleet security officer, who told them that it was a cipher machine similar to the Navy's.

At 8:45 p.m. that night, Thursday, December 4, the watch officer of the F.C.C.'s Radio Intelligence Division telephoned the Office of Naval Intelligence to ask if it could accept a certain message. The O.N.I. officer was not sure and said he would call back. At 9:05 GY watch officer Brotherhood called the F.C.C. and was given a Japanese weather report that sounded like something the F.C.C. man had been told to listen for. He read it to Brotherhood: "Tokyo: today—wind slightly stronger, may become cloudy tonight; tomorrow-—slightly cloudy and fine weather. Kanagawa prefecture: today—north wind cloudy; from afternoon—more clouds. Chiba prefecture: today—north wind clear, may become slightly cloudy. Ocean surface: calm."

Brotherhood was relieved that it included nothing about EAST WIND RAIN, which would have meant the United States, but in any case this message seemed to lack something that would have been required in a true execute. For one thing, the phrase NORTH WIND CLOUDY, which would have meant Russia, was not repeated twice. Nevertheless, Brotherhood telephoned Rear Admiral Leigh Noyes, director of naval communications, who remarked that he thought the wind was blowing from a funny direction. The concensus was that it was not a genuine execute, and the search continued.

In Tokyo, where it was December 5, Foreign Minister Togo received representatives of the Army and Navy general staffs. A general and an admiral wanted to discuss the delicate matter of the precise timing of Japan's final note to the United States. Drafted in English by the director of the Foreign Office's American bureau, the note had been approved by the Liaison Conference, a six-man war cabinet, at its meeting the day before. It rejected Hull's offer of the 26th and concluded: "The Japanese Government regrets to have to notify hereby the American Government that in view of the attitude of the American Government it cannot but consider that it is impossible to reach an agreement through further negotiations."

Article I of the 1907 Hague Convention governing the laws of war provides that ". . . hostilities . . . must not commence without previous and explicit warning, in the form either of a reasoned declaration of war or of an ultimatum with conditional declaration of war." Togo had suggested to the Liaison Conference that the note was far stronger than an ultimatum and that to include a specific declaration of war would be "merely to reiterate the obvious." The conferees had gratefully acceded to this casuistry, since it enabled them to comply with the prior-notification requirement without endangering the surprise of the attack. Since the Hague Convention does not specify how long in advance such notification

must be given, Premier Tojo and the other conferees thought to shave the time as much as possible. Dawn in Hawaii was about noon m Washington. The Liaison Conference had tentatively set 12:30 p.m., Sunday, December 7 (Washington time), as the time of delivery of the note.

But when the two military men called upon Togo the next day to fix the exact time, Vice Admiral Seiichi Ito, vice chief of the naval general staff, told the foreign minister [Togo later wrote] "that the high command had found it necessary to postpone presentation of the document thirty minutes beyond the time previously agreed upon, and that they wanted my consent thereto. I asked the reason for the delay, and Ito said that it was because he had miscalculated. ... I inquired further what period of time would be allowed between notification and attack; but Ito declined to answer this, on the plea of operational secrecy. I persisted, demanding assurance that even with the hour of delivery changed from twelve-thirty to one there would remain a sufficient time thereafter before the attack occurred; this assurance Ito gave. With this—being able to learn no more—I assented to his request. In leaving, Ito said: 'We want you not to cable the notification to the Embassy in Washington too early.'" In this demand lay the seeds of Japan's juridical culpability.

Yoshikawa, in Honolulu, had continued sending his ship-disposition reports after the switch to PA-K2. They were an odd melange of accuracy, error, and outright falsehoods. On December 3, for example, he correctly reported that the liner *Lurline* had arrived from San Francisco but stated that a military transport had departed when no such thing had occurred. The next day he informed Tokyo about the hasty departure of a cruiser of the *Honolulu* class; no such ship either entered or cleared the harbor on the 4th. Then, on the 5th, he cabled that three battleships had arrived in Pearl Harbor, making a total—which he reported with deadly accuracy—of eight anchored in the harbor. His messages, sent over Kita's signature, were decoded in the Foreign Office and routed to the North American section, where Toshikazu Kase passed them immediately to the Navy Ministry. Here they were redrafted, encoded in a naval code, and transmitted on a special frequency not normally used by the Navy and without any direct address to the Pearl Harbor strike force. Commander Koshi decoded it and brought to his chief this latest information.

The communication-security precautions paid off. Whether or not the messages slipped by the American radio monitors in Hawaii mattered little. Mere interception would not have helped much. The messages bore no external indication of their intended recipient, and they could not have been read. Rochefort's attack on Japanese naval codes had achieved some minor successes in late October and November, but he could read only about 10 per cent of the naval traffic, and much of this

consisted of weather and other minor systems. The information obtained, Rochefort said, "was not in any sense vital." Cavite was spottily reading JN25 messages—which revealed nothing about Pearl Harbor—until December 4, when the superencipherment was suddenly changed. As a message that moved on the monitor channel put it: "Five numeral intercepts subsequent to zero six hundred today indicate change of cipher system including complete change differentials and indicator subtracters X All intercepts received since time indicated checked against all differentials three previous systems X No dupes." Corregidor was not to get the initial break into the new superencipherment until December 8. And the only other system in which the Yoshikawa messages might have been forwarded—the flag officers' system—remained unsolved.

A possibility of warning was opened at the source, however, when Yoshikawa's original messages became available to Rochefort's unit. Mayfield had picked up another batch of cables in the surreptitious fashion from Street on Friday morning and immediately sent them down to Rochefort's unit by messenger. Solving them was not part of its duty,[4] but when a superior officer and colleague asks one to do a favor, it is hard to say no. Rochefort assigned the messages to Chief Radioman Farnsley C. Woodward, 39, who had had some experience with Japanese diplomatic codes at the Shanghai station from 1938 to 1940. He had some help from Lieutenant Commanders Thomas H. Dyer, Rochefort's senior cryptanalyst, and Wesley A. Wright, Dyer's assistant. Although the unit was not working on the diplomatic systems, it had information on them in the Navy's R.I.P.s, or Radio Intelligence Publications, with which all radio intelligence units were supplied. The R.I.P. gave, however, only the PA code list, leaving the onerous reconstruction of the current K2 transposition to the cryptanalyst. The half-dozen or so dispatches, plus some in LA, reached Woodward about 1:30 or 2 p.m. Friday, and he immediately began the first of a series of 12- and 14-hour days to read them. He had no difficulty with the LA messages, which were translated into English by Marine Corps Captain Alva Lasswell, but these yielded "nothing but junk." The K2, however, eluded him, and he worked on it far into the night.

In Tokyo it was a little after 1 p.m. on Saturday, December 6. The Japanese reply to Hull's note of the 26th had recently been sent to the cable room of the Foreign Ministry for transmission to the embassy in Washington. Kazuji Kameyama, the cable chief, broke it into fourteen approximately equal parts to facilitate handling and ordered these enciphered on the 97-shiki O-bun In-ji-ki. He also enciphered a shorter "pilot" message from Togo alerting the embassy that the reply was on the way and instructing it "to put it in nicely drafted form and make every preparation to present it to the Americans just as soon as you receive

instructions." At 8:30 p.m., the pilot message was telegraphed from the cable room to Tokyo's Central Telegraph Office, from where, 45 minutes later, it was radioed to the United States. Bainbridge Island intercepted it and relayed it to OP-20-G. By five minutes past noon on Saturday, December 6 (Washington time), OP-20-o had delivered the teletype copy to S.I.S., which promptly ran it through the PURPLE machine. By 2 p.m. Bratton had it, translated and typed. An hour later it was in the hands of the Army distributees. S.I.S. had officially closed at 1 p.m. and was not due to reopen until 6, when it was to go on 24-hour status. But this notification of the imminent receipt of the long-awaited reply to Hull's note of the 26th led to telephoning employees Mary J. Dunning and Ray Cave about 2:30 and asking them to report to work. By 4 both were there.

In Tokyo, Kameyama had released the first 13 parts of the Japanese note to the Central Telegraph Office. Following the instructions of the American bureau, he retained the crucial 14th part, which broke off negotiations. Shortly after 10 p.m., commercial radio began sending the 13 parts to Washington. Most of them took less than ten minutes to transmit, but even though two transmitters were used, it was not until two minutes before 2 a.m. that the tail of the last part had gone. Bainbridge, of course, was listening, and it picked the parts up in this order: 1, 2, 3, 4, 10, 9, 5, 12, 7, 11, 6, 13, 8. One batch arrived by teletype at OP-20-G at eleven minutes before noon, Saturday, December 6, Washington time, and the other at nine minutes of 3 that afternoon. Though it was Saturday, December 6, an even date and hence an Army date of responsibility, the Navy handled the dispatches because it knew that S.I.S. was not expected to work that afternoon, and it considered the intercepts of great importance. Decryptment did not go very smoothly, however. Something seemed to be in error. GY knew the key, but it was producing garbles every few letters. The cryptanalysts tried to correct them.

Meanwhile, a decode into Japanese of the long PA-K2 message that Yoshikawa had sent concerning Kuhn's visual-signal system for Hawaii was placed on the desk of Mrs. Edgers in GZ. "At first glance," she said, "this seemed to be more interesting than some of the other messages I had in my basket, and so I selected it and asked one of the other men, who were also translators working on other messages, whether or not this shouldn't be done immediately and was told that I should and then I started to translate it. Well, it so happened that there was some mistake in the message that had to be corrected and so that took some time. That was at 12:30 or perhaps it was a little before or after 12:30; whatever time it was, we were to go home. It being Saturday, we worked until noon. I hadn't completed it, so I worked overtime and finished it, and I would say that between 1:30 and 2 was when I finished my rough draft translation." Mrs. Edgers left it in the hands of Chief Yeoman Bryant. But

the message was still not entirely clear, and she had not yet had enough experience for her translations to be sent out without further checking. Kramer, busy with the 13 parts, did not examine it in detail.

To speed processing of the 13 parts, GY, learning that some people were in S.I.S., sent over parts 1 and 2. But when Major Doud of S.I.S. ordered Miss Cave to OP-20-G to help in the smooth typeups, the two parts were returned to GY for solution there, probably because of the garbles. But other messages also coming in were retained by S.I.S.

At 3 o'clock, Kramer, in GZ, had checked with GY to find out whether any more Tokyo traffic had come in before releasing his translators for the day. Since the critical matter of a diplomatic note is often found in the last sentences, GY broke down the last part intercepted for him. The first part of the first line indicated in Japanese that this was part 8 of a 14-part message. After about three lines of Japanese text in the preamble, the message came out in English, just as the Foreign Office had sent it. Kramer could let his translators go home. Interspersed throughout the English text were many of the three-letter codewords indicating punctuation, paragraphing, and numbering, but these posed no problem since they had been recovered long ago.

At 4 o'clock, when Linn took over the GY watch, the garbles still had not been cleared. He decided to start from the very beginning, to check the key, find what was wrong, and redecrypt the messages rather than to try to guess at the garbled letters and possibly make serious errors that would distort the sense. Discarding all the previous work caused a serious jam on the Navy's one PURPLE machine, and about 6 p.m. GY again called on S.I.S. for help. Parts 9 and 10 were sent over; an hour later, the decrypts came back in longhand. By 7:30, the last of the 13 parts was being decrypted.

Not all the garbles had been scrubbed out. Part 3 had a 75-letter smudge that could not be read at all, Part 10 a 45-letter blur, and Part 11 one of 50 letters. Part 13 went awry in two patches. One deciphered as *andnd* and the other as *chtualylokmmtt;* GY thought the first should be *and as* and the second *China, can but.*[5]

In the Japanese embassy, about a mile away, the code clerks had completed deciphering the first seven or eight parts of the message by dinnertime. Then they all repaired to the Mayflower Hotel for a farewell dinner for Hidenari Terasaki, head of Japanese espionage for the western hemisphere, who had been ordered to another post.

While they were enjoying themselves, American code clerks at the Department of State were at work encoding a personal appeal for peace from the President of the United States to the Emperor of Japan. This had been off again, on again since October, Roosevelt apparently wishing

to save it for a last resort. Now he decided that the time had come. The message was on its way by 9 o'clock. It traversed the 7,000 miles to Tokyo in an hour.

But it took ten hours to get from the Central Telegraph Office to the American embassy.

As the President was addressing a message of peace to the Emperor, the men of the Japanese strike force were listening to a message of war. Shortly before, Admiral Nagumo had topped off the fuel tanks of his combat ships for the final dash. His crews waved farewell to the slow-moving tankers. Now the officers read a stirring message from Yamamoto to all hands: "The moment has arrived. The fate of the empire is at stake. Let every man do his best." Banzais rent the air. Up the mast of *Akagi* fluttered the very flag that had flown at Japan's great naval victory over Russia in 1905. It was a moment of great emotion. Nagumo altered course to due south and bent on 26 knots. Through a mounting sea, the battle force plunged toward its target.

Lovely, peaceful, that target lay "open unto the fields, and to the sky," oblivious to the onrushing armada of destruction. And as it increased its speed, more information for its mission was starting on its way. The R.C.A. office was time-stamping "1941 Dec 6 PM 6 01" on a message from the consulate. It was signed "Kita" but it came from Yoshikawa. It was brief (only 44 groups) and cheap ($6.82), but it reported that "(1) On the evening of the 5th, the battleship *Wyoming* and one sweeper entered port. Ships at anchor on the 6th were: 9 battleships, 3 minesweepers, 3 light cruisers, 17 destroyers. Ships in dock were: 4 light cruisers, 2 destroyers. Heavy cruisers and carriers have all left. (2) It appears that no air reconnaissance is being conducted by the fleet air arm." Yoshikawa was, as usual, partly right and partly wrong. He mistook *Utah* for *Wyoming.* His figure on the battleships was correct, but in harbor that afternoon were 6 light and 2 heavy cruisers, 29 destroyers, 4 minesweepers, 8 minelayers, and 3 seaplane tenders. With this message Yoshikawa completed his assignment. It was the last cable sent by the Japanese consulate in Hawaii for many years.

[Codebreakers 050.jpg]

*On the eve of Pearl Harbor, Takeo Yoshikawa sends his final message over Consul Kita's signature, using the* PA-K2 *code, to report that the U.S. fleet is still in port*

By 8:45 p.m. in Washington, the 13 parts had been typed in smooth copies and put up in folders. Kramer began telephoning the recipients to

find out where they were so he could bring the MAGIC to them. He also called his wife, Mary, who agreed to chauffeur him during his deliveries. They reached the White House first, at about 9:15. The naval aide, Beardall, had told the President that some MAGIC would be delivered that evening, and at about 4 p.m. he had ordered his communications assistant, Lieutenant Lester R. Schulz, to stand by and bring it to the President. Schulz was waiting in Beardall's small office in the corner of the basement mail room in the White House when Kramer arrived. The Roosevelts had been entertaining at a large dinner party, but the President had excused himself. Schulz obtained permission to bring the MAGIC to the President, and an usher accompanied him to the oval study on the second floor and announced him. Roosevelt was seated at his desk. Only Harry Hopkins was with. him. Schulz unlocked the briefcase with the key that Beardall had given him, removed the sheaf of MAGIC, and handed it to the President. He read the 13 parts in about ten minutes while Hopkins paced slowly up and down. Then Hopkins read them. The 13th part rejected Hull's offer, and when Hopkins had passed the papers back to the President, Roosevelt turned to him and said, in effect, "This means war." Hopkins agreed, and for about five minutes they discussed the situation, the deployment of Japanese forces, the movement towards Indochina, and similar matters. The President mentioned his message to Hirohito. Hopkins remarked that it was too bad that the United States could not strike the first blow and prevent any kind of surprise in the inevitable war.

"No," the President said in effect, "we can't do that. We are a democracy and a peaceful people." He raised his voice: "But we have a good record." He tried unsuccessfully to get Admiral Stark on the telephone, deciding against having him paged at the National Theater for fear of causing undue alarm.

The President then returned the papers to Schulz and, about half an hour after he had entered the study, Schulz left. He found Kramer seated at one of the long tables in the mail room. Schulz gave him the pouch and soon thereafter went home. Kramer, however, continued to the Wardman Park Hotel, where Secretary Knox had a suite. For about twenty minutes, while Kramer chatted with Mrs. Knox and the acting manager of Knox's *Chicago Daily News,* the Secretary read the 13 parts. He agreed with Kramer, that, even incomplete, it pointed to a termination of negotiations. He went into another room to make some telephone calls, and when he came out he told Kramer to bring the latest MAGIC to a meeting that had been arranged for 10 a.m. the next morning with Stimson and Hull in the State Department. (Bratton had delivered the 13 parts to the night duty officer at State at 10 p.m., admonishing him to get them to Hull at once.) Knox returned the intercepts to Kramer, who then went to the home of Rear Admiral Theodore S. Wilkinson, director of naval intelligence, where Beardall and Army intelligence chief Brigadier

General Sherman Miles happened to be dinner guests. All three studied the intercept in a room away from the other guests, Beardall reading from an extra copy that Kramer had. They too seemed to feel that negotiations were coming to an end.

It was after midnight when Kramer left the Wilkinson house. His wife drove him back to the Navy Department, where he put the MAGIC back in his safe in GZ and checked to see if the 14th part had yet come in. It had not. Finally he went home himself.

In S.I.S., meanwhile, the new teletype that would expedite the forwarding of intercepts was being set up in the "cage," the barred room where PURPLE traffic was processed. Monitor Post 2 was requested to send in some intercepts as a test. In San Francisco, Harold W. Martin, the noncom in charge, punched onto the teletype tape the intercepts that the post had picked up since airmailing in the bulk of the day's material, as well as the earlier ones. Among the later ones was Yoshikawa's final message, which thus became one of the first to move on the direct wire as a real, nontest item. S.I.S. received it a little after midnight. But PA-K2 was a low-priority system, and the message had originated in a consular office. It was set aside to be worked on later.

Besides, S.I.S. had more important things to worry about. Like OP-20-O, it was going frantic in a search for the 14th part. Captain Robert E. Schukraft, head of the intercept section, and Frank B. Rowlett, the civilian cryptanalyst in charge of the Japanese diplomatic solutions, checked and rechecked to see whether one of the stations had picked it up and had somehow neglected to forward it. The message preambles had said that it existed, but they could find no trace of it. Neither suspected that the Japanese Foreign Office had deliberately held up transmission of this final conclusive part for security's sake.

Neither did the code clerks at the Japanese embassy. They had returned from Terasaki's party about 9:30, and by midnight had completed deciphering of the 13 parts. While they waited for the final section, they busied themselves by disposing of the remnants of the cipher machine they had destroyed the night before. But they did nothing to fulfill the orders of the pilot message to prepare the dispatch for immediate presentation.

Finally, fourteen hours after the last part of the previous 13 parts had been transmitted, the Foreign Office released the crucial 14th part that broke off negotiations. At 4 p.m., Tokyo time, it ordered it transmitted via both R.C.A. and Mackay Radio & Telegraph Company to ensure its correct reception. An hour and a half later, it wired to the Central Telegraph Office the coded message ordering the 1 p.m. delivery of the 14-part note. This too was sent via the two companies.

As usual, the indefatigable ear of Bainbridge Island detected the

ethereal pulses of both messages. It picked up the Mackay transmission of the 14th part between 12:05 and 12:10 a.m., December 7, local time, and the even briefer one o'clock message between 1:28 and 1:37 a.m. It teletyped them to GY in a single transmission, the 14th part as serial No. 380 of Station S, the one o'clock as No. 381. Brotherhood, who was GY watch officer, ran them through the PURPLE machine. He evidently had some trouble with the 14th part, for it took an hour to break. But by 4 a.m. he had it in English. The three-letter codegroups were quickly translated into punctuation; the message would need little more than typing. The one o'clock message, however, turned out to be in Japanese. He sent it to S.I.S. for translation, knowing that translators were on duty because S.I.S. was beginning its round-the-clock tours. It was a little past 5 a.m., Washington time.

In the embassy of Nippon, the code clerks who had waited all through the night for the 14th part were, on Counselor Iguchi's advice, being sent home. Just as they were climbing wearily into their beds, the naval attaché arrived and found the mailbox stuffed with cablegrams. The duty officer telephoned the clerks at their homes about 8 a.m. and ordered them back to work.

A few hundred miles north of Oahu, the Japanese task force, bristling with guns, planes, and hate for Americans, bore down on the Pacific Fleet. A few hours earlier, a message had arrived from Tokyo that caused Commander Mitsuo Fuchida, the pilot who was to head the first wave of the air attack, to breathe a sigh of relief. It had been relayed from Yoshikawa, and it reported that no barrage balloons had yet been emplaced to protect the fleet from air attack. The same message also caused Commander Minoru Genda to sigh with relief. It stated that the battleships appeared not to be protected by torpedo nets. Genda had conceived the plan of shallow-water torpedo attack on the anchored American ships.

A little more than an hour after the hands of Honolulu clocks had snipped off December 6 and opened out into the first hours of December 7, the Pearl Harbor strike force received Tokyo's relay of Yoshikawa's final message. The American ships were still in harbor, awaiting the ax stroke with fat complacency. They were apparently not even protected by air search. Was it all a decoy? The strike force's radio officer, Commander Kanjiro Ono, listened intently to Honolulu's radio station KGMB for any inkling that the Americans knew of them. He heard only the soft melodies of the islands. On *Hiryu,* the flight deck officer slipped bits of paper between each plane's radio transmitter key and its contact point to make sure that radio silence, so carefully preserved for almost two weeks, would not be accidentally broken in the last few hours to destroy the element of surprise.

As Yoshikawa's final report was being decoded aboard *Akagi,* Kramer returned to the Navy Department he had left only seven hours before, and began working again. It was 7:30 on the morning of Sunday, December 7.

Brotherhood's decryptment of the 14th part was on his desk when he arrived. It took him about half an hour to ready a smooth version, and at 8 o'clock he delivered the neatly typed copy to McCollum. Other copies went to S.I.S. for its distribution. Kramer then worked on other traffic in his office, interrupting himself only once, at 8:45, to bring a copy of the 14th part to naval intelligence chief Wilkinson on his arrival at the Navy Department. At 9:30 he set out to deliver the full 14 parts to the meeting of the three secretaries. He stopped at the office of the Chief of Naval Operations to make sure that Stark had been given the message, which he had, and then walked and trotted to the White House. He got there at about 9:45 and gave the MAGIC pouch to Beardall, who had assigned himself to duty that morning because he thought the 14th part of the message that be had seen at Wilkinson's house the night before might be coming in.

Beardall brought the folder to the President, who was

in his bedroom. Roosevelt said good morning to him, read the intercept, and commented that it looked like the Japanese were going to break off negotiations. Then he returned the MAGIC, and Beardall took it back to the Navy Department.

Kramer, meanwhile, had hurried across the west lawn of the White House to the ugly, ornate State Department building, arriving at about ten minutes of 10. The Army courier appeared at almost the same moment with the MAGIC for Hull and Stimson. Three State Department officials who saw MAGIC—Hornbeck, Ballantine, and Hamilton—were shown the 14th part by Hull's aide, John Stone, and the group discussed the situation in general terms until the secretaries arrived a few minutes later. Kramer gave his pouch to Knox and headed back to the Navy Department.

Meanwhile, the translation of the one o'clock message had come up from S.I.S. It was placed in Bratton's hands about 9 a.m. while he was reading the 14th part. It "immediately stunned me into frenzied activity because of its implications, and from that time on I was busily engaged trying to locate various officers of the general staff and conferring with them on the exclusive subject of this message and its meaning," he said later. He tried first to get in touch with Marshall, calling him at his quarters at Fort Myer, and was told by an orderly that the chief of staff had gone on his customary Sunday morning horseback ride. Bratton directed the orderly:

"Please go out at once, get assistance if necessary, and find General Marshall, ask him to—tell him who I am and tell him to go to the nearest telephone, that it is vitally important that I communicate with him at the earliest practicable moment." The orderly said he would. Bratton called Miles, told him of the message, and urged him to come down to the office at once. Between 10 and 10:30, Marshall called Bratton back. The colonel offered to drive out at once with the one o'clock message, but Marshall told him not to bother, that he was coming down to his office at once. Bratton obeyed.

Kramer arrived back in GZ at about 10:20, and found there the one o'clock message. It struck him as forcibly as it had Bratton. He at once had Yeoman Bryant prepare a new set of folders for immediate delivery of the intercept. Included in the new set were other messages which

S.I.S. had decrypted, and on which Kramer had been working earlier in the morning: Tokyo serial No. 904, which directed the ambassadors not to use an ordinary clerk in preparing the 14-part ultimatum for presentation to the Secretary of State, so as to preserve maximum security; serial No. 909, thanking the two ambassadors for all their efforts; and serial No. 910, ordering destruction of the remaining cipher machine and all machine codes.

Kramer was about to dart out again when Pering, the GY watch officer, brought in a message in plain-language Japanese, ending with the telltale STOP that indicated it was an INGO DENPO message: KOYANAGI RIJIYORI SEIRINOTUGOO

**ARUNITVKI HATTORI MINAMI KINEBUNKO SETURITU KIKINO KYOKAINGAKU SKYUU DENPOO ARITASI STOP TOGO. Kramer**

recognized KOYANAGI as the codeword for *England,* and HATTORI as a codeword whose meaning he did not recall. He consulted his code list and saw that it meant *Relations between Japan and {name of country) are not in accordance with expectation.* But in his haste he overlooked that the common Japanese word *minami,* which means "south," had an INGO DENPO meaning of *U.S.A.* He interpreted the message as "Please have director Koyagani send a wire stating the sum which has been decided to be spent on the South Hattori Memorial Library in order that this business may be wound up." Consequently, he dictated a decode that omitted *United States: Relations between Japan and England are not in accordance with expectation.* Yeoman Bryant inserted this and three other minor messages that had come over from the Army into the folders. Kramer meanwhile made a navigator's time circle that indicated that one o'clock in Washington was dawn in Hawaii and the very early hours of the morning in the Far East around Singapore and the Philippines, which everybody seemed to be watching. He shoved the folders into the briefcase and dashed out the door.

He went first to Stark's office, where the officers were discussing the 14th part, summoned McCollum, gave him the pouch that included the final code-destruction and one o'clock messages, and mentioned to him the significance of the latter's timing. McCollum grasped it at once and disappeared into Stark's office. Kramer wheeled and hurried down the passageway. He emerged from the Navy Department building and turned right on Constitution

Avenue, heading for the meeting in the State Department three or four blocks away. The urgency of the situation washed over him again, and he began to move on the double.

He half trotted, half walked to State, getting there at about 10:45. Hull, Knox, and Stimson were still meeting. Kramer saw them grouped around the conference table when the door to Hull's office was opened briefly. He gave the MAGIC messages to Stone, explaining to him how the one o'clock time of delivery of the ultimatum tied in with the movement of a big Japanese convoy down the coast of Indochina, and mentioning in passing that the time in Hawaii would be 7:30 a.m. The final code-destruction message was self-explanatory. Kramer carried a MAGIC pouch to the White House, and then returned, perspiring, to the Navy Department, to busy himself with still more MAGIC. At about 12:30, he spotted the omission of *United States* from the INGO DENPO message. Because the one o'clock meeting was so close, he telephoned the recipients with the correction, a practice he had followed several times in the past, but reached only McCollum and Bratton. He told them that *United States* was to be inserted in file number 7148. The force of it had been considerably lessened by the one o'clock message, but Kramer, conscientious beyond the basic requirements of duty, nevertheless planned to send around a corrected version.

Safford later estimated that OP-20-G handled three times as much material that weekend as on a normal one; the GY log shows at least 28 messages in PURPLE alone handled that Sunday. And these messages were processed much more expeditiously than at any other time in the past, Kramer said. The cryptanalysts had done their duty, and had done it superbly. Events now passed out of their hands.

In Tokyo, the President's message to the Emperor had finally been delivered to Grew after a delay of ten hours. The chief of the censorship office had ordered that all foreign cables be held up for five hours one day and ten hours the next. The order had been issued at the request of a lieutenant colonel on the general staff, who asked that this be done "as a precaution." The President's "triple priority" message arrived on one of the ten-hour days, was stalled for the required time, and was finally delivered at 10:30 p.m., Tokyo time.

Grew immediately arranged for a meeting with Togo and, when the message had been decoded, drove to Togo's official residence at 12:15 a.m. He requested—as is the right of all ambassadors—an audience with the head of state to present the message, then read it aloud to Togo and gave him a copy. Togo promised to present the matter to the Throne and, despite the lateness of the hour, telephoned the Lord Keeper of the Privy Seal for an audience. Ministers of state would be received at any hour,

and the audience was arranged for 3 a.m. Togo began having the message translated.

It was then about 5:30 a.m., December 7, in Hawaii. The Japanese task force was only 250 miles north of Pearl Harbor. More than 2,000 Americans with less than three hours to live slept or played in blissful ignorance of that fact. The hands of clocks in the Foreign Office in Tokyo, in the code room at the Japanese embassy in Washington, in the War and Navy departments, in Pearl Harbor, circled around and around, but not so quickly as the spinning propellers of Nagumo's ships. At 5:30, two cruisers catapulted off a pair of scout planes to make sure the Americans were still there.

The clerks at the embassy had straggled back to work between 9:30 and 10. They began decoding the longer cables first, as experience had shown that these were usually the more important. At the same time, the embassy's first secretary, Katzuso Okumura, was typing up the first 13 parts of the ultimatum. He had been chosen because the Foreign Office had forbidden the use of an ordinary typist in the interests of secrecy and he was the only senior official who could operate a typewriter at all decently. At about 11:30, code clerk Juichi Yoshida adjusted the Alphabetical Typewriter to the proper keys and typed out a short code message. To the consternation of the entire staff, it turned out to be an instruction to deliver the 14-part message to Secretary Hull at 1 p.m., Washington time. The 14th part had not even been decoded from the sheaf of incoming cables! And only one code machine was left to decipher all the messages!

A few blocks away, General Marshall had just arrived at the War Department. On his desk was the MAGIC folder with the 14-part message on top and the one o'clock message under it. He began to read the ultimatum carefully, some parts several times. Bratton and Brigadier General Leonard T. Gerow, the war plans chief, tried to get him to look at the one o'clock message, but it is rather difficult for subordinates to interrupt a four-star general, and he finished the ultimatum before finding the time-of-delivery message. It struck him with the same sense of urgency that it had the others, and he picked up the telephone to call Stark to see if he wanted to join him in sending a warning message to American forces in the Pacific.

At approximately the same time, Ambassador Nomura was calling Hull to request an appointment at 1 p.m. And 230 miles north of Hawaii, the first wave of Japanese planes was thundering off the flight decks of the carriers.

Stark was at that moment discussing the significance of the one

o'clock message with Captain R. E. Schuirman, Navy's liaison with State. He told Marshall that he felt that enough warnings had been sent and that more would just confuse the commanders. Marshall thereupon wrote out the dispatch he wanted sent:

> Japanese are presenting at one p.m. Eastern Standard Time today what amounts to an ultimatum also they are under orders to destroy their code machine immediately Stop Just what significance the hour set may have we do not know but be on alert accordingly Stop

On his desk Marshall had a scrambler telephone with which he could have called Short in Hawaii. The scrambling apparatus stood in a room next to his office, thus obviating the possibility of tapping the conversation in unscrambled form, as was done in commercial cases. But Marshall knew that scramblers afforded protection merely against casual listeners; they could be penetrated by a determined eavesdropper with proper equipment. He had on several occasions warned the President about security on his transatlantic telephone conversations with Ambassador Bullitt in France and later with Churchill—a wise move, for, though he did not know it, the Nazis had already penetrated that scrambler. The Japanese had evidenced some interest in the San Francisco-Honolulu scrambler, and Marshall was acutely sensitive "that the Japanese would have grasped at most any straw" to suggest to the isola-

tionists that the administration had committed an overt act that had forced the Japanese hand. Japanese interception of a scrambler warning might thus have sent the country to war divided. So Marshall shunned the scrambler telephone and relied on the slightly slower but much more secure method of enciphering a written message.

As he was completing the message, Stark called him back. He had reconsidered and wanted Marshall to add the usual admonition to show the message to the naval opposites. Marshall added: "Inform naval authorities of this communication." Stark offered the Navy communication facilities, but Marshall said that the Army's could get the message out as quickly.

Marshall gave the message to Bratton to take it to the War Department message center for transmission to the commanding generals in the Philippines, Hawaii, the Caribbean, and West Coast, after vetoing a suggestion that it be typed first. As Bratton was leaving, Gerow called out that if there was any question as to priority, to send it to the Philippines first. Bratton, greatly agitated, gave the message to Colonel Edward French in the message center and asked how long it would take to get it out. French told him that it would be encoded in three minutes, on the air in eight, and in the hands of the addressees in twenty. Bratton returned and reported to Marshall, who did not understand the explanation and sent him back for a clarification. He still was not sure and sent Bratton back a third time, after which he was finally satisfied with the answer.

Meanwhile, French had had the message typed anyway and then ordered it encoded on a machine that was operated from a typewriter keyboard. During the few minutes that this took, he checked his Honolulu circuit, and found that since early morning interference had been so bad that the small 10-kilowatt War Department radio could not "bust" through it. He knew that R.C.A. in San Francisco had a 40-kilowatt transmitter which would have no difficulty in getting through, and that Western Union in San Francisco had a tube running across the street from its office to this R.C.A. office. He had also learned on the previous day that R.C.A. was installing a teletype circuit from its office in Honolulu to Short's headquarters at Fort Shafter. French figured that this would therefore be his most expeditious route; after the message had been

encoded, he personally carried it over to his bank of six Western Union teletypes and, at 12:01 p.m. December 7, sent it on its way. Western Union forwarded it at 12:17, and 46 minutes later it was received by R.C.A. in Honolulu. Local time was 7:33 a.m. The first wave of Japanese planes was then only 37 miles away—so close that the Army radar operators at Opana Point, who had tracked the flight for several hours and had been told to "Forget it" when they first reported it, were about to lose it in the dead zone of the nearby hills. But though the teletype connection for Fort Shatter had been completed the day before, it was not in operation pending tests on Monday. R.C.A. put Marshall's message in an envelope marked "Commanding General" for hand delivery.

In Tokyo, Togo had been received by the Emperor. He read the text of Roosevelt's message, then a draft of the imperial reply that he and Tojo had prepared. It stated that the 14-part note was to be considered as Japan's response. Hirohito assented, and at 3:15 a.m. Togo withdrew from the Divine Presence. Deeply moved, he recalled, "I passed solemnly, guided by a Court official, down several hundred yards of corridors, stretching serene and tranquil. Emerging at the carriage entrance of the Sakashita Gate, I gazed up at the brightly shining stars, and felt bathed in a sacred spirit. Through the Palace plaza in utter silence, hearing no sound of the sleeping capital but only the crunching of the gravel beneath the wheels of my car, I pondered that in a few short hours would dawn one of the eventful days of the history of the world." Even as he pondered, Japanese planes were circling over Pearl Harbor.

In stark contrast to the calm stillness of Tokyo was the hectic bustle of the Japanese embassy on Massachusetts Avenue.

Soon after the one o'clock message had been decoded, Okumura finished typing the first 13 parts. But he decided that this rough draft did not suit the formality of a document to be delivered to the Secretary of State. He began retyping it from the very beginning, being assisted now by a junior interpreter, Enseki. His task was complicated by two messages sent up from the code room, one ordering the insertion of a sentence that had been accidentally

dropped, one changing a word. This required the retyping of several pages, including one just completed with a great deal of trouble. At about 12:30, the code room finally gave him the 14th part of the ultimatum, but Okumura was nowhere near finished with the first 13. Nomura kept poking his head in the door to hurry him on. A few minutes after one, when it was evident that the document would not be finished for some time, the Japanese called Hull to request a postponement to 1:45, saying that the document they wished to present was not yet ready. Hull acquiesced.

At almost exactly the time that the call to Hull was being placed, Commander Fuchida and his flight of 51 dive bombers, 49 high-level bombers, 40 torpedo planes, and 43 fighters arrived over Pearl Harbor. He fired a "black dragon" from his signal pistol to indicate that the squadrons should deploy in the assault pattern for complete surprise. Nine minutes later, he wirelessed the message "To, to, to"—the first syllable of the Japanese word for "Charge!" and the signal to attack. As the planes moved into position for their runs, he felt so certain that he had achieved complete surprise that, at 7:53, two minutes before the first bomb even fell, he jubilantly radioed "TORA! TORA! TORA!" ("Tiger! Tiger! Tiger!")—the prearranged codeword that indicated surprise. On *Akagi,* Nagumo turned to a brother officer and grasped his hand in a long, silent handshake. At 7:55, the first bomb exploded at the foot of the seaplane ramp at the southern end of Ford Island in the middle of Pearl Harbor.

Okumura was still typing. His fingers struggled with the keys as torpedoes capsized *Oklahoma,* as bombs sank *West Virginia,* as 1,000 men died in the searing inferno of *Arizona.* At 1:50 p.m. Washington time, 25 minutes after the attack had started, he reached the end of his typing marathon. The two ambassadors, who were waiting in the vestibule, started for the State Department as soon as it was handed to them.

The Japanese envoys arrived at the Department at 2:05 and went to the diplomatic waiting room [Hull wrote]. At almost that moment the President telephoned me from the White House. His voice was steady but clipped.

He said, "There's a report that the Japanese have attacked Pearl Harbor."

"Has the report been confirmed?" I asked.

He said, "No."

While each of us indicated his belief that the report was probably true, I suggested that he have it confirmed, having in mind my

appointment with the Japanese Ambassadors. . . .

Nomura and Kurusu came into my office at 2:20. I received them coldly and did not ask them to sit down.

Nomura diffidently said he had been instructed by his Government to deliver a document to me at one o'clock, but that difficulty in decoding the message had delayed him. He then handed me his Government's note.

I asked him why he had specified one o'clock in his first request for an interview.

He replied that he did not know, but that was his instruction.

I made a pretense of glancing through the note. I knew its contents already but naturally could give no indication of this fact.

After reading two or three pages, I asked Nomura whether he had presented the document under instructions from his Government.

He replied that he had.

When I finished skimming the pages, I turned to Nomura and put my eye on him.

"I must say," I said, "that in all my conversations with you during the last nine months I have never uttered one worth of untruth. This is borne out absolutely by the record. In all my fifty years of public service I have never seen a document that was more crowded with infamous falsehoods and distortions— infamous falsehoods and distortions on a scale so huge that I never imagined until today that any Government on this planet was capable of uttering them."

Nomura seemed about to say something. His face was impassive, but I felt he was under great emotional strain. I stopped him with a motion of my hand. I nodded toward the' door. The Ambassadors turned without a word and walked out, their heads down.

The warlords' hopes of shaving the warning time to the closest possible margin had quite literally gone up in the smoke of attack, and Japan had 'started hostilities without giving prior notification. Later, this failure to declare war would be made part of the charges on which the Japanese war criminals were tried—and convicted, some of them paying with their lives. Togo would try to exonerate himself by throwing the blame on the embassy personnel for neglecting to decipher the cables promptly and to type the ultimatum at once. Perhaps some lawyer's talking point might have been salvaged if the ambassadors had grabbed Okumura's original copy, no matter how messy, and taken it to Hull at 1 p.m., or if they had taken the first few pages of the fair copy at 1 p.m. and directed the embassy staff to rush the other pages over as completed. But even if the entire document had been delivered on time, the 25 minutes that remained until the attack would not have been sufficient time for all the steps needed to prevent surprise: reading the document, guessing that a military attack was intended, notifying the War and Navy departments, composing, enciphering, transmitting, and deciphering an appropriate warning, and alerting the outpost forces. This was just what the shoguns intended. But just as a multitude of human errors on the part of Americans, cascading one atop the other, helped make tactical surprise perfect, so a series of similar human errors on the part of the Japanese deprived them of their last vestige of legality.

Shortly after the attack commenced, Tadao Fuchikama, a messenger for the Honolulu office of R.C.A., picked up a batch of cables for delivery. He knew that the war had started and that it was the Japanese who were attacking the ships in the harbor, but he felt he had his job to do anyway. He glanced at the addresses on the envelopes, including the one marked "Commanding General," and planned an efficient route. Shafter was well down the list. His motorcycle progressed slowly through the jammed traffic; once he was stopped by National Guardsmen who had almost taken him for a paratrooper. At 11:45, almost two hours after the last attackers had vanished, Marshall's warning message was delivered to the signal officer. It got to the decoding officer at 2:40 that afternoon and to Short himself at 3. He took one look at it and threw it into the wastebasket, saying that it wasn't of the slightest interest.

In Tokyo, Grew was awakened at 7 a.m. by the tele-

phone, summoning him to a meeting at 7:30 with Togo. On Grew's arrival, the Foreign Minister gave him the Emperor's reply to the President. He thanked Grew for his cooperation and saw him off at the door. Four hours had elapsed since the attack had begun, but Togo never mentioned it. Shortly thereafter, Grew learned of the outbreak of hostilities from an extra of the *Yomiuri Shimbun* hawked outside his window. The Japanese soon closed the embassy gates.

The Japanese in Washington destroyed their last machine and codes after encoding a final message that they were so doing—the last message sent on the Washington-Tokyo circuit, and read, of course, by the American codebreakers. But in Honolulu, police guarding the consulate after the attack smelled papers burning and saw smoke coming from behind a door. Fearing a conflagration, they broke in and found the consulate staff burning its remaining documents in a washtub on the floor. The police confiscated what proved to be the telegraph file plus five burlap sacks full of torn papers. These reached Rochef ort's unit that evening. Woodward was still working long hours in an attempt to break the PA-K2 messages that Mayfield had brought. Since the attack, the fear of sabotage had swelled to enormous proportions. "Nothing coming to light," his notes read, "so it was decided to reverse the process of deciphering, allowing for the encoding party to have either purposely encrypted the messages in this manner or possibly to have made an error in using the system employed due to confusion. This netted results."

At about 2 a.m. on December 9, he cracked one of the messages picked up in the consulate. It was one sent from the Foreign Ministry to Kita on the 6th: "Please wire immediately re the latter part of my #123 any movements of the fleet after the 4th." With this, he was soon able to unlock the other PA-K2 messages—including the long one setting up Kühn's light-signaling system. At about the same time in OP-20-oz, Kramer, who had been too busy with the 13 parts on Saturday to work on this message, was breaking out charts of Oahu and Maui to help in de-garbling the message, which was finally reduced to plaintext by Thursday. Marshall later said that it was the first message that clearly indicated an attack on Pearl to him— but this was, of course, after the fact.

**From: Tokyo**

**To: Washington**

**7 December 1941**

**#902 Part 14 of 14**

**(Note: In the forwarding instructions to the radio station handling this part, appeared the plain English phrase "VERY IMPORTANT")**

**7. Obviously it is the intention of the American Government to conspire with Great Britain and other countries to obstruct Japan's efforts toward the establishment of peace through the creation of a New Order in East Asia, and especially to preserve Anglo-American rights and interests by keeping Japan and China at war. This intentiona has been revealed clearly during the course of the present negotiations. Thus the earnest hope of the Japanese Government to adjust Japanese-American relations and to preserve and promote the peace of the Pacific through cooperation with the American Government has finally been lost.**

**The Japanese Government regrets to have to notify hereby the American Government that in view of the attitude of the American Government it cannot but consider that it is impossible to reach an agreement through further negotiations.**

**JD-1:7143 SECRET (M) Navy trans. 7 Dec 1941 (S-TT)**

*The fourteenth part of the Japanese ultimatum, as distributed to* MAGIC *recipients*

The information from it was immediately passed to counterintelligence units in Hawaii, where invasion was thought highly probable. Their agents interrogated residents in the neighborhood of the houses mentioned in the dispatch and listened to recordings of KGMB want ads, but found that the signal system had never been used. They arrested Kühn, who confirmed this. He was convicted on espionage charges and imprisoned at Leavenworth Penitentiary until after the war, when he was paroled to leave the country.

On December 7, while Honolulu was still reeling from the devastation of the attack, F.C.C. monitors there picked up a Japanese-language news broadcast from station jzi in Japan. The announcer boasted of a "death-defying raid" at Pearl, reported other events, and, about halfway through the broadcast, declared: "Allow me to especially make a weather forecast at this time: west wind clear."

and China at war. This intention has been revealed clearly during the course of the present negotiation. Thus, the earnest hope of the Japanese Government to adjust Japanese-American relations and to preserve and promote the peace of the Pacific through cooperation with the American Government has finally been lost.

The Japanese Government regrets to have to notify hereby the American Government that in view of the attitude of the American Government it cannot but consider that it is impossible to reach an agreement through further negotiations*

December 7, 1941.

*The last page of the Japanese note as typed by First Secretary Katzuso Okwnura and handed to Secretary of State Cordell Hull while Pearl Harbor was being attacked*

The O.N.I. translator noted that "as far as I can recollect, no such Weather forecast has ever been made before" and that "it may be some sort of code." It was the long-awaited winds code execute, apparently sent indicating war with Britain to make sure that some Japanese outpost that had not reported destroying its codes by the codeword HARUNA Would burn them.

Shortly after noon in Washington on the day after the attack, the President of the United States stood before a stormily applauding joint session of Congress and opened a black looseleaf notebook. When the cheers had subsided into a hushed solemnity, he began to speak:

> Yesterday, December 7, 1941—a date which will live in infamy—the United States of America was suddenly and deliberately attacked by naval and air forces of the Empire of Japan.

He alluded to the fatal Japanese delay in delivering the ultimatum:

> The United States was at peace with that nation and, at the solicitation of Japan, was still in conversation with its Government and its Emperor looking toward the maintenance of peace in the Pacific. In deed, one hour after Japanese air squadrons hac commenced bombing in Oahu, the Japanese Ambas sador to the

United States and his colleague delivered to the Secretary of State a formal reply to a recen American message. While this reply stated that i seemed useless to continue the existing diplomats negotiations, it contained no threat or hint of war 01 armed attack.

The war was on. The most treacherous onslaught it history had succeeded. Japan had cloaked the strike fores in absolute secrecy. She had dissembled with diplomatic conversations and with jabs toward the south. She had—ir a precaution whose wisdom she but dimly realized—swathed her plans in a communications security so all enveloping that not a whisper of them ever floated ont< the airwaves.

But if the cryptanalysts had no chance to warn of th< attack and save American lives before the war, they foum ample opportunities to exert their subtle and pervasivr talents during the struggle. In the 1,350 days of conflici in which an angry America turned Japan's tactical victory at Pearl Harbor into total strategic defeat, the cryptanalysts, in the words of the Joint Congressional Committee, "contributed enormously to the defeat of the enemy, greatly shortened the war, and saved many thousands of lives."

That, however, is another story.

## 3. The First 3,000 Years

ON A DAY nearly 4,000 years ago, in a town called Menet Khufu bordering the thin ribbon of the Nile, a master scribe sketched out the hieroglyphs that told the story of his lord's life—and in so doing he opened the recorded history of cryptology. His was not a system of secret writing as the modern

world knows it; he used no fully developed code of hieroglyphic symbol substitutions. His inscription, carved about 1900 B.C. into the living rock in the main chamber of the tomb of the nobleman Khnumhotep II, merely uses some unusual hieroglyphic symbols here and there in place of the more ordinary ones. Most occur in the last 20 columns of the inscription's 222, in a section recording the monuments that Khnumhotep had erected in the service of the pharaoh Amenemhet II. The intention was not to make it hard to read the text. It was to impart a dignity and authority to it, perhaps in the same way that a government proclamation will spell out "In the year of Our Lord One thousand eight hundred and sixty three" instead of just writing "1863." The anonymous scribe may also have been demonstrating his knowledge for posterity. Thus the inscription was not secret writing, but it incorporated one of the essential elements of cryptography: a deliberate transformation of the writing. It is the oldest text known to do so.

As Egyptian civilization waxed, as the writing developed and the tombs of the venerated dead multiplied, these transformations grew more complicated, more contrived, and more common. Eventually the scribes were replacing the usual hieroglyphic form of a letter, like the full-face mouth representing /r/, by a different form, like a profiled mouth. Sometimes they used new hieroglyphs whose first sound represented the letter desired, as a picture of a pig, "rer," would mean /r/. Sometimes the sounds of the two hieroglyphs differed but their images resembled one another. The horned asp, representing *HI,* was replaced by the serpent, representing /z/. And sometimes the scribes used a hieroglyph on the rebus principle, as in English a picture of a bee might represent *b;* thus a sailboat, "khentey," stands for another Egyptian word *khentey,* which means "who presides at"—this latter being part of a title of the god Amon, "he who presides at Karnak." These procedures °f acrophony and the rebus are essentially those of ordinary Egyptian writing; it was through them that the hieroglyphics originally acquired their sound values. The Egyptian transformations merely carry them further, elaborate them, and make them more artificial.

The transformations occur in funerary formulas, in a hymn to Thoth, in a chapter of the Book of the Dead, on the sarcophagus of the pharaoh Seti I, in royal titles dis-

played in Luxor, on the architrave of the Temple of Luxor, on stele, in laudatory biographic inscriptions. There is nothing meant to be concealed in all this; indeed, many of the statements are repeated in ordinary form right next to the altered ones. Why, then, the transformations? Sometimes for essentially the same reason as in Khnumhotep's tomb: to impress the reader. Occasionally for a calligraphic or decorative effect; rarely, to indicate a contemporary pronunciation; perhaps even for a deliberate archaism as a reaction against foreign influence.

But many inscriptions are tinctured, for the first time, with the second essential for cryptology—secrecy. In a few cases, the secrecy was intended to increase the mystery and hence the arcane magical powers of certain religious texts. But the secrecy in many more cases resulted from the understandable desire of the Egyptians to have passersby read their epitaphs and so confer upon the departed the blessings written therein. In Egypt, with its concentration upon the afterlife, the number of these inscriptions soon • proliferated to such an extent that the attention and the goodwill of visitors flagged. To revive their interest, the scribes deliberately made the inscriptions a bit obscure. They introduced the cryptographic signs to catch the reader's eye, make him wonder, and tempt him into unriddling them — and so into reading the blessings. It was a sort of Madison Avenue technique in the Valley of the Kings. But the technique failed utterly. Instead of interesting the readers, it evidently destroyed even the slightest desire to read the epitaphs, for soon after the funerary cryptography was begun, it was abandoned.

[Codebreakers 070.jpg]

The addition of secrecy to the transformations produced cryptography. True, it was more of a game than anything else—it sought to delay comprehension for only the shortest possible time, not the longest—and the cryptanalysis was, likewise, just a puzzle. Egypt's was thus a quasi cryptology in contrast to the deadly serious science of today. Yet great things have small beginnings, and these hieroglyphs did include, though in an imperfect fashion, the two elements of secrecy and transformation that comprise the essential attributes of the science. And so cryptology was born.

In its first 3,000 years, it did not grow steadily. Cryptology arose independently in many places, and in most of them it died the deaths of its civilizations. In other places, it survived, embedded in a literature, and from this the next generation could climb to higher levels. But

progress was slow and jerky. More was lost than retained. Much of the history of cryptology of this time is a patchwork, a crazy quilt of unrelated items, sprouting, flourishing, withering. Only toward the Western Renaissance does the accreting knowledge begin to build up a momentum. The story of cryptology during these years is, in other words, exactly the story of mankind.

China, the only high civilization of antiquity to use ideographic writing, seems never to have developed much real cryptography—perhaps for that reason. In one case known for military purposes, the 11th-century compilation, *Wu-ching tsung-yao* ("Essentials from Military Classics"), recommended a true if small code. To a list of 40 plaintext items, ranging from requests for bows and arrows to the report of a victory, the correspondents would assign the first 40 ideograms of a poem. Then, when a lieutenant wished, for example, to request more arrows, he was to Write the corresponding ideogram at a specified place on an ordinary dispatch and stamp his seal on it.

In China's great neighbor to the west, India, whose civilization likewise developed early and to high estate, several forms of secret communications were known and, [a]Pparently, practiced. The *Artha-sastra,* a classic work on statecraft attributed to Kautilya, in describing the espionage service of India as practically riddling the country with [s]Pies, recommended that the officers of the institutes of [£]spionage give their spies their assignments by secret writ-

ing. Perhaps most interesting to cryptologists, amateur or professional, is that Vatsyayana's famous textbook of erotics, the *Kama-sutra,* lists secret writing as one of the 64 arts, or yogas, that women should know and practice. The fourth great civilization of antiquity, the Mesopo-tamian, rather paralleled Egypt early in its cryptographic evolution, but then surpassed it. Thus, in the last period of cuneiform writing, in colophons written at Uruk (in present-day Iraq) under the Seleucid kings in the last few score years before the Christian era, occasional scribes converted their names into numbers. The encipherment—if such it be—may have been only for amusement or to show off.

The Holy Scriptures themselves have not escaped a touch of cryptography—or protocryptography, to be precise, for the element of secrecy is lacking.

Hebrew tradition offers at least two such conversions in the Old Testament (none are recorded for the New). In Jeremiah 25:26 and 51:41, the form SHESHACH appears in place of *Babel* ("Babylon"). The second occurrence strikingly demonstrates the lack of a secrecy motive, since the phrase with SHESHACH is immediately followed by one using "Babylon":

How is Sheshach taken! And the praise of the whole earth seized! How is Babylon become an astonishment Among the nations!

Confirmation that SHESHACH is really a substitute for *Babel* and not a wholly separate place comes from the Septuagint and the Targums, the Aramaic paraphrases of the Bible, which simply use "Babel" where the Old Testament version has SHESHACH. The second transformation, at Jeremiah 51:1, puts LEB KAMAI ("heart of my enemy") for *Kashdim* ("Chaldeans").

Both transformations resulted from the application of a traditional substitution of letters called "atbash," in which the last letter of the Hebrew alphabet replaces the first, and vice versa; the next-to-last replaces the second, and vice versa; and so on. It is the Hebrew equivalent of *a* = *z, b* — Y, *c* = x,. . . , z = A.

[Codebreakers 073.jpg]

Consequently, in *Babel,* the repeated *b,* or *beth,* the second letter of the Hebrew alphabet, became the repeated SH, or SHIN, the next-to-last letter, in SHESHACH. Similarly, the /, or *lamed,* became the hard CH, or KAPH. The *kaph* of *Kashdim* reciprocally became the LAMED of LEB KAMAI. In this

determination, the Hebrew letters sin and shin, which differ only by where a dot is placed, are regarded as the same letter. The only letters in Hebrew are consonants and two silent letters, aleph and ayin; vowels are represented by dots or lines, usually below the letters. What is a final i in the English LEB KAMAI is a letter YOD in Hebrew, whose atbash reciprocal is *mem.* The word "atbash," incidentally, derives from the very procedure it denotes, since it is composed of aleph, taw, beth, and shin—the first, last, second, and next-to-last letters of the Hebrew alphabet.

Both SHESHACH and LEB KAMAI have considerably embarrassed biblical commentators. They have devised numerous ingenious explanations for why so odd a result as LEB KAMAI would be desired, or why secrecy was wanted. Some have even thought Sheshach the name of a Babylonian district. But the idea of simple scribal manipulation, which would mean that such desires never even existed, and which is advanced by modern authorities and bolstered by the similar examples from other cultures and by the predilection of scribes for amusing themselves with word and alphabet games, seems the best explanation.

"Queen Anteia, Proetus's wife, had fallen in love with the handsome youth," the "incomparable Bellerophon . . . who was endowed with every manly grace, and begged him to satisfy her passion in secret." So Homer begins the story in the *Iliad* that includes the world's first conscious reference to—as distinct from use of—secret writing.

"But Bellerophon was a man of sound principles and refused. So Anteia went to King Proetus with a lying tale. 'Proetus,' she said, 'Bellerophon has tried to ravish me. Kill him—or die yourself.' The king was enraged when he

heard this infamous tale. He stopped short of putting Bellerophon to death—it was a thing he dared not do—but he packed him off to Lycia with sinister credentials from himself. He gave him a folded tablet on which he- had traced a number of devices with a deadly meaning, and told him to hand this to his father-in-law, the Lycian king, and thus ensure his own death."

The Lycian king feasted Bellerophon for nine days. "But the tenth day came, and then, in the first rosy light of Dawn, he examined him and asked to see what credentials he had brought him from his son-in-law Proetus. When he had deciphered the fatal message from his son-in-law, the king's first step was to order Bellerophon to kill the Chimera," a fire-breathing monster with a lion's head, a goat's body, and a serpent's tail. Bellerophon did. The Lycian king then tried one ruse after another to carry out the surreptitious instructions, but Bellerophon successively battled the Solymi, defeated the Amazons, and slew the best warriors of Lycia, who had ambushed him. In the end the Lycian king relented, realizing that the youth stood under the divine protection of the gods, and gave him his daughter and half his kingdom.

This is the only mention of writing in the *Iliad.* Homer's language is not precise enough to tell exactly what the markings on the tablets were. They were probably nothing more than ordinary letters—actually substitution of symbols for letters seems too sophisticated for the era of the Trojan War. But the mystery that Homer throws around the tablets does suggest that some rudimentary form of concealment was used, perhaps some such allusion as "Treat this man as well as you did Glaucus," naming someone whom the king had had assassinated. The whole tone of the reference makes it fairly certain that here, in the first great literary work of European culture, *appear* that culture's first f aint glimmerings of secrecy in communication.

A few centuries later, those glimmerings had become definite beams of light. Several stories in the *Histories of* Herodotus deal specifically with methods of steganography (not cryptography). The Father of History tells how one of the most important messages in the history of Western civilization was transmitted secretly. It gave to the Greeks the crucial information that Persia was planning to conquer them. According to Herodotus,

> The way they received the news was very remark-bale. Demaratus, the son of Ariston, who was an exile in Persia, was not, I imagine—and as is only natural to suppose—well disposed toward the Spartans; so it is open to question whether what he did was inspired by benevolence or malicious pleasure. Anyway, as soon as news reached him at Susa that Xerxes had decided upon

> the invasion of Greece, he felt that he must pass on the information to Sparta. As the danger of discovery was great, there was only one way in which he could contrive to get the message through: this was by scraping the wax off a pair of wooden folding tablets, writing on the wood underneath what Xerxes intended to do, and then covering the message over with wax again. In this way the tablets, being apparently blank, would cause no trouble with the guards along the road. When the message reached its destination, no one was able to guess the secret until, as I understand, Cleomenes' daughter Gorgo, who was the wife of Leonidas, discovered it and told the others that, if they scraped the wax off, they would find something written on the wood underneath. This was done; the message was revealed and read, and afterwards passed on to the other Greeks.

The rest is well-known. Thermopylae, Salamis, and Plataea ended the danger that the flame of Western civilization would be extinguished by an Oriental invasion. The story is not without a certain bitter irony, however, for Gorgo, who may be considered the first woman cryptanalyst, in a way pronounced a death sentence on her own husband: Leonidas died at the head of the heroic band of Spartans who held off the Persians for three crucial days at the narrow pass of Thermopylae.

It was the Spartans, the most warlike of the Greeks, who established the first system of military cryptography. As early as the fifth century B.C., they employed a device called the "skytale," the earliest apparatus used in cryptology and one of the few ever devised in the whole history of the science for transposition ciphers. The skytale consists of a staff of wood around which a strip of papyrus or leather or parchment is wrapped close-packed. The secret message is written on the parchment down the length of the staff; the parchment is then unwound and sent on its way. The dis-

connected letters make no sense unless the parchment is rewrapped around a baton of the same thickness as the first; then words leap from loop to loop, forming the message.

Thucydides tells how it enciphered a message from the ephors, or rulers, of Sparta, ordering the too-ambitious Spartan prince and general Pausanius to follow the herald back home from where he was trying to ally himself with the Persians, or have war declared against him by the Spartans. He went. That was about 475 B.C. About a century later, according to Plutarch, another skytale message recalled another Spartan general, Lysander, to face charges of insubordination.

Another Greek writer, Polybius, devised a system of signaling that has been adopted very widely as a cryptographic method. He arranged the letters in a square and numbered the rows and columns. To use the English alphabet, and merging / and /' in a single cell to fit the alphabet into a 5 X 5 square:

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 1 | a | b | c | d | e |
| 2 | f | g | h | ij | k |
| 3 | l | m | n | o | p |
| 4 | q | r | s | t | u |
| 5 | v | w | x | y | z |

Each letter may now be represented by two numbers—that of its row and that of its column. Thus *e* = 15, v = 51. Polybius suggested that these numbers be transmitted by means of torches—one torch in the right hand and five in the left standing for *e,* for example. This method could signal messages over long distances. But modern cryptographers have found several characteristics of the Polybius square, or "checkerboard," as it is now commonly called, exceedingly valuable—namely, the conversion of letters to numbers, the reduction in the number of different characters, and the division of a unit into two separately manipulable parts. Polybius' checkerboard has therefore become very widely used as the basis of a number of systems of encipherment.

Polybius and others never said whether any of the substitution ciphers they described were actually used, and so the first attested use of that genre in political affairs come

*j>v\j\j* j A^r

from the Romans — and from the greatest Roman of them all. Julius Caesar thus impressed his name permanently into cryptology.

Suetonius, the gossip columnist of ancient Rome, says that Caesar wrote to Cicero and other friends in a cipher in which the plaintext letters were replaced by letters standing three places further down the alphabet, D for *a,* E for *b,* etc. Thus, the message *Omnia Gallia est divisa in partes tres* would be enciphered (using the modern 26-letter alphabet) to RPQLD JDOOLD HVW GLYLVD LQ SDUWHV WUHV. To this day, any cipher alphabet that consists of the standard sequence, like Caesar's:

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *Plain* | a | b | c | d | e | f | g | h | I | j | k | l | m |
| *Cipher* | D | E | F | G | H | I | J | K | L | M | N | O | P |
| *Plain* | n | o | p | q | r | s | t | u | v | w | x | y | z |
| *Cipher* | Q | R | S | T | U | V | W | X | Y | Z | A | B | O |

is called a Caesar alphabet, even if it begins with a letter other than D.

It must be that as soon as a culture has reached a certain level, probably measured largely by its literacy, cryptography appears spontaneously — as its parents, language and writing, probably also did. The multiple human needs and desires that demand privacy among two or more people in the midst of social life must inevitably lead to cryptology wherever men thrive and wherever they write. Cultural diffusion seems a less likely explanation for its occurrence in. so many areas, many of them distant and isolated.

The Yezidis, an obscure sect of about 25,000 people in, northern Iraq, use a cryptic script in their holy books because they fear persecution by their Moslem neighbors. Tibetans use a kind of cipher called "rin-spuns" for official correspondence; it is named for its inventor Rin-c'(hhen-) spuns(-pa), who lived in the 1300s. The Nsibidi secret society of Nigeria keeps its pictographic script from Europeans as much as possible because it is used chiefly to express love in rather direct imagery, and samples appear to be at least as pornographic as they are cryptographic. The cryptography of Thailand developed under Indian influence. An embryonic study of the subject even appears in a grammatical work entitled *Poranavakya* by Hluang Prasot Aksaraniti (Phe). One system, called "the erring Siamese," substitutes one delicate Siamese letter for another. In an-

other system, consonants are divided into seven groups of five letters; a letter is indicated by writing the Siamese number of its group and placing vertical dots under it equal in number to the letter's place in its group. A system called "the hermit metamorphosing letters" writes the text backwards.

[Codebreakers 078.jpg]

In the Europe of the Latin alphabet—from which modern cryptology would spring—cryptography flickered weakly. With the collapse of the Roman empire, Europe had plunged into the obscurity of the Dark Ages. Literacy had all but disappeared. Arts and sciences were forgotten, and cryptography was not excepted. Only during the Middle Ages occasional manuscripts, with an infrequent signature or gloss or "deo gratias" that a bored monk put into cipher to amuse himself, fitfully illuminate the cryptologic darkness, and, like a single candle guttering in a great medieval hall, their feeble flarings only emphasize the gloom.

The systems used were simple in the extreme. Phrases

were written vertically or backwards; dots were substituted for vowels; foreign alphabets, as Greek, Hebrew, and Armenian, were used; each letter of the plaintext was replaced by the one that follows it; in the most advanced system, special signs substituted for letters. For almost a thousand years, from before 500 to 1400, the cryptology of Western civilization stagnated.

During all these years, cryptology was acquiring a taint that lingers even today—the conviction in the minds of many people that cryptology is a black art, a form of occultism whose practitioner must, in William F. Friedman's apt phrase, "perforce commune daily with dark spirits to accomplish his feats of mental jiu-jitsu."

In part it is a kind of guilt by association. From the early days of its existence, cryptology had served to obscure critical portions of writings dealing with the potent subject of magic—divinations, spells, curses, whatever conferred supernatural powers on its sorcerers. Another important factor was the confusion of cryptology with the Jewish kabbalah.

But, important as all these were, the view that cryptology is black magic in itself springs ultimately from a superficial resemblance between cryptology and divination. Extracting an intelligible message from ciphertext seemed to be exactly the same thing as obtaining knowledge by examining the flight of birds, the location of stars and planets, the length and intersections of lines in the hand, the entrails of sheep, the position of dregs in a teacup. In all of these, the wizard-like operator draws sense from grotesque, unfamiliar, and apparently meaningless signs. He makes known the unknown.

All this stained cryptology so deeply with the dark hues of esoterism that some of them still persist, noticeably coloring the public image of cryptology. People still think cryptanalysis mysterious. Book dealers still list cryptology under "occult." And in 1940 the United States conferred upon its Japanese diplomatic cryptanalyses the codename MAGIC.

In none of the secret writing thus far was there any sustained cryptanalysis. Occasional cases, yes. But of any science of cryptanalysis, there was nothing. Only cryptography existed. And therefore cryptology, which involves

both cryptography and cryptanalysis, had not yet come into being so far as all these cultures—including the Western —were concerned.

Cryptology was born among the Arabs. They were the first to discover and write down the methods of cryptanalysis. The people that exploded out of Arabia in the 600s and flamed over vast areas of the known world swiftly engendered one of the highest civilizations that history -had yet seen. Science flowered. Arab medicine and mathematics became the best in the world—from the latter, in fact, comes the word "cipher." Practical arts flourished. Administrative techniques developed. The exuberant creative energies of such a culture, excluded by its religion from painting or sculpture, and inspired by it to an explication of the Holy Koran, poured into literary pursuits. Storytelling, exemplified by Sheherazade's *Thousand and One Nights,* word-riddles, rebuses, puns, anagrams, and similar games abounded; grammar became a major study. And included was secret writing.

The Arabic knowledge of cryptography was fully set forth in the section on cryptology in the *Subh al-a 'sha,* an enormous, 14-volume encyclopedia written to afford the secretary class a systematic survey of all the important branches of knowledge. It was completed in 1412 and succeeded in its task. Its author, who lived in Egypt, was Shihab al-DIn abu '!-'Abbas Ahmad ben 'Ali ben Ahmad 'Abd Allah al-Qalqashandi. The cryptologic section, "Concerning the concealment of secret messages within letters," has two parts, one dealing with symbolic actions and allusions, the other with invisible inks and cryptology. Qalqashandi attributed most of his information on cryptology to the writings of Taj ad-Din 'All ibn ad-Duraihim ben Muhammad ath-Tha'alibi al-Mausill, who lived from 1312 to 1361 and held various teaching and official posts under the Mamelukes in Syria and Egypt. Except for a theological treatise, none of his writings is extant, but he is reported to have authored two works on cryptology.

After explaining that one may write in an unknown language to obtain secrecy, Ibn ad-Duraihim, according to Qalqashandi, gave seven systems of ciphers. This list encompassed, for the first time in cryptography, both transposition and substitution ciphers. Moreover, one system is the first known cipher ever to provide more than one substitute for a plaintext letter. Remarkable and important

as this is, however, it is overshadowed by what follows— the first exposition on cryptanalysis in history.

It appeared in full maturity in Qalqashandi's paraphrase of Ibn ad-Duraihim, but its beginnings are probably to be found in the intense and minute scrutiny of the Koran by whole schools of grammarians in Basra, Kufa, and Baghdad to elucidate its meanings. Among other studies, they counted the frequency of words to attempt a chronology for the chapters of the Koran, certain words being considered as having been used only in the later chapters. Lexicography advanced this. In making a dictionary, considerations of letter-frequency and of which letters go or do not go together virtually thrust themselves upon the lexicographer. For example, the Arabs recognized early that za' was the rarest letter in Arabic and, contrariwise, that the omnipresence of the definite article "al-" made alif and lam the most common letters in normal style.

The Ibn ad-Duraihim—Qalqashandi exposition begins at the beginning: the cryptanalyst must know the language in which the cryptogram is written. Because Arabic, "the noblest and most exalted of all languages," is "the one most frequently resorted to" (in that part of the world), there follows an extensive discussion of its linguistic characteristics. Lists are given of letters that are never found together in one word, of letters that rarely come together in a word, of combinations of letters that are not possible ("Thus tha' may not precede shin."), and so on. Finally, the exposition gives a list of letters in order of "frequency of usage in Arabic in the light of what a perusal of the Noble Koran reveals." The writers even note that "In non-Koranic writings, the frequency may be different from this." Following which, Qalqashandi explains lucidly the principles of cryptanalysis and demonstrates with two examples. But this knowledge vanished in the Arab decline.

The technique of cryptanalysis rests on two phenomena. One is that all letters are not used equally in any language. In other words, the first 26 letters of say, the Gettysburg Address do not contain one *a,* one *b,* one *c,* so on. Rather, some letters occur more often than others. The second phenomenon is that the proportions in which the letters occur remain constant. If 1,000 letters of the Gettysburg Address are counted and compared with 1,000 letters of a military dispatch and 1,000 of a sports story, the counts will show that in all three texts certain letters—always the

same letters—will appear frequently. Other Jetters will appear very rarely in all three texts, and some letters will appear occasionally. Since these texts are all English, *e* will be the most frequent letter. The vowels *a, o, i,* and the consonants *t, n, r, s,* and *h* will also be of high frequency, while /', *k, q, x* and *z* will be of low frequency. This constancy suggests that a frequency count of the next text will show the same letters with the same frequencies—everi if that text happens to be concealed by a cipher system. The cryptanalyst can utilize the known frequencies to dislodge the text from the cipher.

In other words, given a monoalphabet substitution whose plaintext he knows to be in English, the cryptanalyst will count the number of letters in the ciphertext. If he finds that, say, L is the most frequent, he knows by the nature of the cipher that it must stand for the most frequent letter in the hidden plaintext. Since that is English, he can expect that that letter is *e.* Consequently, he can assume that L represents *e.* This is the basic process of cryptanalysis.

The process of identification continues through other letters. Usually in English *t* is the second most frequent letter, and it might well represent the second most frequent ciphertext letter. But frequency characteristics are not limited to individual letters. They extend to letter combinations. Thus in English the vowels *a, i,* and *o* associate relatively seldom with one another. The cryptanalyst, examining his statistics and finding three high-frequency letters that avoid one another, could assume that they represent the vowels. Then, seeing a ciphertext letter that follows vowels four-fifths of the time and precedes them only one-fifth, he could guess that that letter stands for n, which behaves in just that way. Again, to spot *h* he can use the fact that the combinations *th and he* are among the most common while *ht* and *eh* are relatively rare.

Then he exploits these identifications to make others by deciphering as much of the message as he can with his equivalents and then guessing what the missing letters might be. Suppose that he has recovered *e, t,* and *h.* Inserting these values at one point he finds the partial plaintext *the?e.* He can assume that the missing letter is probably *r or s* and can test these assumptions at other points in the cryptogram. The one that yields intelligible plaintext is the correct one. Thus he continues until the entire cryptogram is solved.

Monoalphabetic substitution is today a trivial form of cipher. But the technique of its solution lies at the heart of the cryptanalysis of nearly all more sophisticated substitution ciphers. Their solution consists in large measure of breaking down the cipher until the method for solving monoalphabetic substitutions can be applied. That method is therefore of fundamental importance.

## 4. The Rise of the West

MODERN WESTERN cryptology emerged directly from the flowering of modern diplomacy. The ambassadors' reports were sometimes opened and read, and, if necessary, crypt-analyzed. By the end of the century, cryptology had become important enough for most states to keep full-time cipher secretaries occupied in making up new keys, enciphering and deciphering messages, and solving intercepted dispatches. Sometimes the cryptanalysts were separate from the cipher secretaries and were called in only when needed. Perhaps the most elaborate organization was Venice's. It fell under the immediate control of the Council of Ten, the powerful and mysterious body that ruled the republic largely through its efficient secret police. Venice owed her preeminence largely to Giovanni Soro, who was perhaps the West's first great cryptanalyst. Soro, appointed cipher secretary in 1506, enjoyed remarkable success in solving the ciphers of numerous principalities. His solution of a dispatch of Mark Anthony Coloana, chief of the army of the Holy Roman Emperor Maximilian I, requesting 20,000 ducats or the presence of the emperor with the army, gave an insight into Colonna's problems. So great was Soro's fame that other courts sharpened their ciphers, and as early as 1510 the papal curia was sending him ciphers that no one in Rome could solve. But Venice had no monopoly.

In 1589, Henry of Navarre, who was destined to become the most popular king in the history of France (he coined the slogan "A chicken in every peasant's pot every Sunday"), ascended to the throne as Henry IV and found himself embroiled still more fiercely in his bitter contest

with the Holy League, a Catholic faction that refused to concede that a Protestant could wear the crown. The League, headed by the Duke of Mayenne, held Paris and all the other large cities of France, and was receiving large transfusions of men and money from Philip of Spain. Henry was tightly hemmed in, and it was at this juncture that some correspondence between Philip and two of his liaison officers, Commander Juan de Moreo and Ambassador Manosse, fell into Henry's hands.

It was in cipher, but he had in his government at the time one Francois Viete, the seigneur de la Bigotiere, a 49-year-old lawyer from Poitou who had risen to become counselor of the parlement, or court of justice, of Tours and a privy counselor to Henry. Viete had for years amused himself with mathematics as a hobby—"Never was a man more born for mathematics," said Tallement des Reaux. As the man who first used letters for quantities in algebra, giving that study its characteristic look, Viete is today remembered as the Father of Algebra. A year before, he had solved a Spanish dispatch addressed to Alessandro Farnese, the Duke of Parma, who headed the Spanish forces of the League. Henry turned the new intercepts over to him to see if Viete could repeat his success.

He could and did. The plaintext of the long letter from Moreo, in particular, was filled with intimate details of the negotiations with Mayenne: ". . . Your Majesty having 66,000 men in those states [the Netherlands], it would be nothing to allot 6,000 to so pressing a need. Should your refusal become known, all will be lost. ... I said nothing about that to the Duke of Parma. . . . The Duke of Mayenne stated to me that it was his wish to become king; I could not hold back my surprise. . . ." The message was couched in a new nomenclator that Philip had specially given Moreo when he departed for France; it consisted of the usual alphabet with homophonic substitutions, plus a code list of 413 terms represented by groups of two or three letters (LO = *Spain;* PUL = *Navarre;* POM = *King of Spain)* or of two numbers, either underlined (64 = *confederation)* or dotted (94 = *Your Majesty). A* line above a two-digit group indicated a null.

Moreo's letter had been dated October 28, 1589, and despite Viete's experience and the quantity of text, it was not until March 15 of the following year that Viete was

able to send Henry the completed solution, though he had previously submitted bits and pieces. What Viete did not know was that, 110 miles from Tours, Henry had defeated Mayenne's superior force at Ivry west of Paris the day before, making the solution somewhat academic.

Any chagrin that Viete felt did not deter him from extending his cryptanalytic successes. As he wrote to Henry in the letter forwarding the Moreo solution: "And do not get anxious that this will be an occasion for your enemies to change their ciphers and to remain more covert. They have changed and rechanged them, and nevertheless have been and always will be discovered in their tricks." It was an accurate prediction, for Viete continued to read the enciphered messages of Spain and of other principalities as well. But his pride led him straight into a trap in which a shrewd diplomat drew confidential information from him as deftly as he elicited the secret meaning from elegant and mysterious symbols. Giovanni Mocenigo, the Venetian ambassador to France, said that he was talking one day with Viete at Tours:

> He [Viete] had just told me that a great number of letters in cipher of the king of Spain as well as of the [Holy Roman] Emperor and of other princes had been intercepted, which he had deciphered and interpreted. And as I showed a great deal of astonishment, he said to me:
>
> "I will give your government effective proofs of it." He immediately brought me a thick packet of letters from the said princes which he had deciphered, and added:
>
> "I want you also to know that I know and translate your cipher."
>
> "I will not believe it," I said, "unless I see it." And as I had three kinds of cipher—an ordinary which I used, a different one which I did not use, and a third, called dalle Caselle—he showed me that he knew the first. Then, to better probe so grave an affair, I said to him,
>
> "You undoubtedly know our dalle Caselle cipher?" "For that, you have to skip a lot," he replied, meaning that he only knew portions of it. I asked him to let me see some of our deciphered letters, and he promised to let me, but since then he has not spoken

further about it to me, and, having left, I have not seen him any more.

Mocenigo was reporting to the Council of Ten, and it was after hearing his remarks that they so promptly replaced their existing keys.

Meanwhile, Philip had learned, from his own interceptions of French letters, that Viete had broken a cipher that the Spanish—who apparently knew little about cryptanaly-sis—had thought unbreakable. It irritated him, and thinking that he would cause trouble for the French at no cost to himself, told the pope that Henry could have read his ciphers only by black magic. But the tactic boomeranged. The pope, cognizant of the ability of his own cryptologist, Giovanni Batista Argenti, and perhaps even aware that papal cryptanalysts had themselves solved one of Philip's ciphers 30 years before, did nothing about the Spaniard's complaint; all Philip got for his effort was the ridicule and derision of everyone who heard about it.

At about the same time, England's first great cryptanalyst helped to execute a sentence of death on that most romantic and tragic of royal ladies, Mary, Queen of Scots.

He was Thomas Phelippes. Son of London's collector of customs, he traveled widely in France in his mid-twenties. As early as 1538, while in Paris, he had begun cryptanalyzing messages for Sir Francis Walsingham, Queen Elizabeth's Satanic-looking minister in charge of espionage. Back in England, Phelippes became one of Walsingham's most confidential assistants. He was an indefatigable worker, corresponding tirelessly in his calligraphic hand with Walsingham's numerous agents. His letters show a fair acquaintance with literary allusions and classical quotations, and he appears to have been able to solve ciphers in Latin, French, and Italian and, less proficiently, in Spanish. The only known physical description of him comes from the pen of Mary of Scots herself, who describes Phelippes, whose hair and beard were blond, as "of low stature, slender every way, eated in the face with small pocks, of short sight, thirty years of age by appearance."

Mary's unflattering comments betrayed her suspicions about Phelippes—suspicions that were well founded. For Phelippes and his master, Walsingham, were casting a jaundiced eye on Mary for reasons that, in their turn, were

equally well founded. Mary was the heir apparent to the throne of England. She was also nominally queen of Scotland, though she had been ejected in a tangled series of - events and had been prevented from returning by the opposition of the strong Protestant party there to her indiscretions. She was a remarkable woman: beautiful, possessed of great personal charm, commanding the loyalty of her subordinates, courageous, unshakably devoted to her religion, but also unwise, stubborn, and capricious. Various Catholic factions had schemed more than once to seat her on the throne of England and so restore the realm to the Church. The chief result had been to confine Mary to various castles in England and to alert Walsingham to seek an opportunity to extirpate once and for all this cancer that threatened to destroy his own queen, Elizabeth.

The opportunity arose in 1586. A former page of Mary's, Anthony Babington, began organizing a plot to have courtiers assassinate Elizabeth, incite a general Catholic uprising in England, and crown Mary. A conspiracy that involved the overthrow of the government naturally had ramifications all over the country, and Babington also gained the support of Philip II, who promised to send an expedition to help, once Elizabeth was safely dead. But the plan depended ultimately on the acquiescence of Mary, and to obtain this Babington had to communicate with her.

This was no easy task. Mary was then being held incommunicado under house arrest at the country estate of Chartley. But a handsome former seminarian named Gilbert Gifford, recruited by Babington as a messenger, discovered a way of smuggling Mary's letters into Chartley in a beer keg. It worked so well that the French ambassador gave Gifford all the correspondence that had been accumulating for Mary for the past two years.

Much of it was enciphered. But this was only part of the care that Mary took to ensure the security of her communications. She insisted that important letters be written within her suite and read to her before they were enciphered. Dispatches had to be sealed in her presence. The actual encipherment was usually performed by Gilbert Curll, her trusted secretary, less often by Jacques Nau, another secretary. Mary not infrequently ordered changes in her nomenclators, which were much smaller and flimsier than the diplomatic ones.

What neither Mary nor Babington knew was that, despite

their elaborate precautions, their correspondence was being delivered to Walsingham and Phelippes as quickly as they wrote it. Gilbert Gifford was a double-agent, a ne'er-do-well who had offered his services to Walsingham. Walsingham, seeing an unparalleled opportunity to insinuate his antennae into Mary's circles, employed Gifford to turn over to him all Mary's letters, which he copied and then passed on. It included the two-year backlog entrusted to Gifford by the French ambassador, and the rapidly growing volume of traffic generated by Babington's festering plot. These enciphered missives were being solved by Phelippes almost as quickly as he got his hands on them. As the conspiracy reached a crescendo of preparation in the middle of July, he was sometimes reading two or more in a day: two letters from the queen bear notations "decifred 18 July 1586," two others are marked as deciphered July 21, and there are still other cipher letters in the same packet in the records that bear no notations.

During these three months, Walsingham cannily made no arrests, but simply let the plot develop and the correspondence accumulate in the hope that Mary would incriminate herself. His expectations were fulfilled. Early in July, Babington specified the details of the plan in a letter to Mary, referring to the Spanish invasion, her own deliverance, and "the dispatch of the usurping competitor." Mary considered her reply for a week and, after composing it carefully, had Curll encipher it; she sent it off to Babington on July 17. It was to prove fatal, for in it Mary acknowledged "this enterprise" and advised Babington of ways "to bring it to good success." Phelippes, on solving it, immediately endorsed it with the gallows mark.

But Walsingham still lacked the names of the six young courtiers who were to commit the actual assassination. So when the letter reached Babington, it bore a postscript that was not on it when it left Mary's hands; in it Babington was asked for "the names and qualities of the six gentlemen which are to accomplish the designment." Both the forgery and the encipherment in the correct key seem to be the work of Phelippes.

It proved unnecessary. Babington needed to go abroad to organize the invasion; at Walsingham's suggestion, there was a mixup in the passports. Babington, suspecting nothing, boldly came to the minister for help in cutting the red tape.

[Codebreakers 089.jpg]

While he was dining at the nearby tavern with one of Walsingham's men, a note came, calling for his arrest. He caught a glimpse of it and,

saying he was going to pay the bar bill and leaving his cloak and sword on the back of his chair, he slipped out and escaped. The hue and cry set up by his pursuers panicked the six young men. They fled for their lives, but within a month both they and Babington were caught and condemned to death after a two-day trial. Before they were executed, the authorities prudently extracted from Babington the cipher alphabets he had used with Mary.

These, and Mary's letters, served as thoroughly incriminatory evidence in the Star Chamber proceedings that convicted her of high treason. Mary received the announcement that Elizabeth had signed her death warrant with majestic tranquillity, and at eight on the morning of February 8, 1587, after eloquently reiterating her innocence and praying aloud for her church, for Elizabeth, for her son, and for all her enemies, mounted the platform with solemn dignity, knelt, and received the axeman's three strokes with the courage that had marked every other action of her life. Thus did Mary, Queen of Scots, exit this transient life and enter the more enduring one of legend, as her motto had prophesied: "In my end is my beginning." There seems little doubt that she would have died before her time, the politics of the day being what they were. But there seems equally little doubt that cryptology hastened her unnatural end.

## 5. On The Origin of a Species

"DATO and I were strolling in the Supreme Pontiff's gardens at the Vatican and we went from topic to topic marveling at the ingenuity that men showed in various enterprises, till Dato gave expression to his warm admiration for those men who can exploit what are called 'ciphers.' "

So wrote Leon Battista Alberti near the beginning of the succinct but suggestive work that earned him the title of Father of Western Cryptology. Alberti was the first of a group of writers who, element by element, developed a type of cipher to which most of today's systems of cryptography belong. The species is polyalphabetic substitution.

It was the amateurs of cryptology who created the species. The professionals, who almost certainly surpassed them in cryptanalytic expertise, concentrated on the down-to-earth problems of the systems that were then in use but are now outdated. The amateurs, unfettered to these realities, soared into the empyrean of theory. There were four whose thought took wings: a famous architect, an intellectual cleric, an ecclesiastical courtier, and a natural scientist.

The architect was Alberti, a man who, perhaps better than anyone except Leonardo da Vinci, epitomizes the Renaissance ideal of the universal man. Born in 1404, the illegitimate but favored son of a family of rich Florentine merchants, Alberti enjoyed extraordinary intellectual and athletic aptitudes. He painted, composed music, and was regarded as one of the best organists of his day. Writings poured from his pen. His *De Re Aedificatoria,* the first printed book on architecture, written while Gothic churches were still being built, helped shape the thoughts of those who built such utterly non-Gothic structures as St. Peter's Basilica in Rome. Jacob Burckhardt, author of the classic *The Civilization of the Renaissaance in Italy,* singled out Alberti as one of the truly all-sided men who tower above their numerous many-sided contemporaries. And another great Renaissance scholar, John Symonds, declared that "He presents the spirit of the 15th century at its very best."

Among his friends was the pontifical secretary, Leonardo Dato, one of the learned men of his age, who during that memorable stroll in the Vatican gardens brought the conversation around to cryptology. "You've always been interested in these secrets of nature," Dato said. "What do you think of these decipherers? Have you tried your hand at it, as much as you know how to?"

Alberti smiled. He knew that Date's duties included ciphers (it was before the curia had a separate cipher secretary). "You're the head of the papel secretariat," he teased. "Could it be that you had to use these things a few times in matters of great importance to His Holiness?"

"That's why I brought it up," Dato replied candidly. "And because of the post I have, I want to be able to do it myself without having to use outside interpreters. For when they bring me letters in cipher intercepted by spies, it's no joking matter. So please—if you've thought up any new ideas having to do with this business, tell me about them." So Alberti promised that he would do some work on it so that Dato would see that it was profitable to have asked him, and the result was the essay that he wrote in 1466 or early 1467, when he was 62 or 63.

He implied that he thought up the idea of frequency analysis all by himself, but the conception that he set forth is far too matured for that. Nevertheless, his remarkably lucid Latin essay, totaling about 25 manuscript pages, constitutes the West's oldest extant text on cryptanalysis.

Only after he had explained how ciphers are solved did he proceed to ways of preventing solution. He capped his work with a cipher of his own invention that he called "worthy of kings" and, like all inventors, claimed was unbreakable. This was the cipher disk that founded poly-alphabeticity. With this invention, the West, which up to this point had equaled but had never surpassed the East in cryptology, took the lead that it has never lost.

"I make two circles out of copper plates. One, the larger, is called stationary, the smaller is called movable. The diameter of the stationary plant is one-ninth greater than that of the movable plate. I divide the circumference of each circle into 24 equal parts. These parts are called cells. In the various cells of the larger circle I write the capital letters, one at a time in red, in the usual order of the letters, A first, B second, c third, and then the rest, omitting H and K [and Y] because they are not necessary." This gave him 20 letters, since j, u, and w were not in his alphabet, and in the remaining four spaces he inscribed the numbers 1 and 4 in black. (The red and black seem to signify only that Alberti liked colors.) In each of the 24 cells of the movable circle he inscribed "a small letter in black, and not in regular order like the stationary characters, but scattered at random.

Codebreakers 092.jpg

Thus we may suppose the first of them to be a, the second g, the third q, and so on with the rest until the 24 cells of the circle are full; for there are 24 characters in the Latin alphabet, the last being et [probably meaning "&"]. After completing these arrangements we place the smaller circle upon the larger so that a needle driven through the centers of both may serve as the axis of both and the movable plate may be revolved around it."

The two correspondents—who, Alberti carefully pointed out, must each have identical disks—agree upon an index letter in the movable disk, say k. Then, to encipher, the sender places this prearranged index letter against any letter of the outer disk. He informs his correspondent of this position of the disk by writing, as the first letter of the ciphertext, this letter of the outer ring. Alberti gave the example of k being placed against B. "From this as a starting point all the other characters of the message will acquire the force and sounds of the stationary characters above them."* So far nothing remarkable had happened. But in his next sentence Alberti placed cryptography's feet on the road to its modern complexity. "After writing three or four words, I shall change the position of the index in our formula by turning the circle, so that the index k may be, say, under D. So in my message I shall write a capital D, and from

this point on [ciphertext] k will signify no longer B but D, and all the other stationary letters at the top will receive new meanings."

There is the crucial point: "new meanings." Each new position of the inner disk brings different letters opposite one another in the inner and outer rings. Consequently, each shift means that plaintext letters would be replaced with different ciphertext equivalents. For example, the plaintext word NO might be enciphered to fc at one setting and to ze at another. Equally, at each shift a given cipher-text letter would stand for a different plaintext letter than it did at the previous setting. Thus, the fc that formerly represented NO might, at the new setting, stand for plaintext TU. This shift in both plain and cipher equivalents dif-

*In Alberti's disk, the outer capital letters are the plaintext and the inner lower-case letters are the ciphertext. This contradicts the convention of this book, and is being used in the section on Alberti only to avoid altering his text. The difference is signalized by not using italic for the lower case.

1

ferentiates polyalphabetic from homophonic or polyphonic substitution.

Each new setting of Alberti's disk brought into play a new cipher alphabet, in which both the plaintext and the ciphertext equivalents are changed in regard to one another. There are as many of these alphabets as there are positions of his disk, and this multiplicity means that Alberti here devised the first polyalphabetic cipher.

This achievement—critical in the history of cryptology —Alberti then adorned by another remarkable invention: enciphered code. It was for this that he had put numbers in the outer ring. In a table he permuted the numbers 1 to 4 in two-, three-, and four-digit groups, from 11 to 4444, and used these as 336 codegroups for a small code. "In this table, according to agreement, we shall enter in the various lines at the numbers whatever complete phrases we please, for example, corresponding to 12, 'We have made ready the ships which we promised and supplied them with troops and grain.' " These code values did not change, any more than the mixed alphabet of the disk did. But the digits resulting from an encoding were then enciphered with the disk just as if they were plaintext letters. In Alberti's words, "These numbers I then insert in my message according to the formula of the cipher, representing them by the letters that denote these numbers." These numbers thus changed their ciphertext equivalents as the disk turned. Hence 341, perhaps meaning "Pope," might become mrp at one position and fco at another. This constitutes an excellent form of enciphered code, and just how precocious Alberti was may be seen by the fact that the major powers of the earth did not begin to encipher their code messages until 400 years later, near the end of the 19th century, and even then their systems were much simpler than this.

Alberti's three remarkable firsts—the earliest Western exposition of cryptanalysis, the invention of polyalphabetie substitution, and the invention of enciphered code—make him the Father of Western Cryptology. But although his treatise was published in Italian in a collection of his works in 1568, and although his ideas were absorbed by papal cryptologists and perhaps influenced the science's development, they never had the dynamic impact that such prodigious accomplishments ought to have produced. Symonds' evaluation of his work in general may both explain why

and summarize the modern view of his cryptological contributions: "This man of many-sided genius came into the world too soon for the perfect exercise of his singular faculties. Whether we regard him from the point of view of art, of science, or of literature, he occupies in each department the position of precursor, pioneer, and indicator. Always original and always fertile, he prophesied of lands he was not privileged to enter, leaving the memory of dim and varied greatness rather than any solid monument behind him."

Polyalphabeticity took another step forward in 1518, with the appearance of the first printed book on cryptology, written by one of the most famous intellectuals of his day. This was Johannes Trithemius, a Benedictine monk whose dabbling in alchemy and other mystic powers made him one of the most revered figures in occult science, while his more solid scholarship won him the title of "Father of Bibiliography." In 1518, a year and a half after his death, his *Polygraphiae libri sex, loannis Trithemii abbatis Peapolitani, quondam Spanheimensis, ad Maximilianum Caesarem* ("Six Books of Polygraphy, by Johannes Trithemius, Abbot at Wurzburg, formerly at Spanheim, for the Emperor Maximilian") was published. By far the bulk of the volume consists of the columns of words printed in large Gothic type that Trithemius used in his systems of cryptography. But in the work's Book V appears, for the first time, the square table, or tableau. This is the elemental form of polyalphabetic substitution, for it exhibits all at once all the cipher alphabets in a particular system. These are usually all the same sequence of letters, but shifted to different positions in relation to the plaintext alphabet, as in Alberti's disk the inner alphabet assumed different positions in regard to the outer alphabet. The tableau sets them out in orderly fashion—the alphabets of the successive positions laid out in rows one below the other, each alphabet shifted one place to the left of the one above. Each row thus offers a different set of cipher substitutes to the letters of the plaintext alphabet at the top. Since there can be only as many rows as there are letters in the alphabet, the tableau is square.

The simplest tableau is one that uses the normal alphabet in various positions as the cipher alphabets. Each cipher alphabet produces, in other words, a Caesar substitution.

This is precisely Trithemius' tableau, which he called his "tabula recta." Its first and last few lines were:

```
abcdefghiklmnopqrstuxyzw
bcdefghiklmnopqrstuxyzwa
cdefghiklmnopqrstuxyzwab
defghiklmnopqrstuxyzwabc
efghiklmnopqrstuxyzwabcd
.......................
zwabcdefghiklmnopqrstuxy
wabodefghiklmnopqrstuxyz
```

Trithemius used this tableau for his polyalphabetic encipherment, and in the simplest manner possible. He enciphered the first letter with the first alphabet, the second with the second, and so on. (He gave no separate plaintext alphabet, but the normal alphabet at the top can serve.) Thus a plaintext beginning *Hunc caveto virum . . .* became HXPF GFBMCZ FUEiB. ... In this particular message, he switched to another alphabet after 24 letters, but in another example he followed the more normal procedure of repeating the alphabets over and over again in groups of 24.

The great advantage of this procedure over Alberti's is that a new alphabet is brought into play with each letter. Alberti shifted alphabets only after three or four words. Thus the ciphertext would mirror the obvious pattern of repeated letters of a word like *Papa* ("Pope"), or in English, *attack,* and the cryptanalyst could seize upon this reflection to break into the cryptogram. The letter-by-letter encipherment obliterates this clue.

If the first two steps in polyalphabeticity were made by men who were giants in their time, the third was taken by a man who was so unexceptional that he left almost no traces. This is Giovan Batista Belaso; the sum total of knowledge about him consists of the facts that he came from Brescia of a noble family, served in the suite of one Cardinal Carpi, and, in 1553, brought out a little booklet entitled *La cifra del. Sig. Giovan Bastista Belaso.* In this he proposed the use of a literal, easily remembered, and easily changed key—he called it a "countersign"—for a poly-alphabetic cipher. Wrote Belaso: "This countersign may consist of some words in Italian or Latin or any other language, and the words may be few or many as desired. Then we take

the words we wish to write, and put them

on paper, writing them not too close together. Then over each of the letters we place a letter of our countersign in this form. Suppose, for example, our countersign is the little versetto VIRTUTI OMNIA PARENT. And suppose we wish to write these words: *Larmata Turchesca partira a cinque di Luglio.* We shall put them on paper in this manner:

```
VIRTUTI OMNIA PARENT VIRTUTI OMNIA PARENT VI
larmata turch escapa rtiraac inque dilugl io"
```

The keyletter that is paired with a given plaintext letter indicates the alphabet of the tableau that is to be used to encipher that plaintext letter. Thus, / is to be enciphered by the V alphabet, *a* by the I alphabet, and so on. The system permits great flexibility: no longer did all messages have to be enciphered with one of a relatively few standard sequences of alphabets, but different ambassadors could be given individual keys, and, if it were feared that a key had been stolen or solved, a new one could be substituted with the greatest of ease. Keys caught on at once, and the Belaso invention laid the foundation for today's exceedingly complex arrangements, in which not one but several keys are employed and are varied at odd intervals. Moreover, in combining the best of his two predecessors—the mixed alphabet of Alberti and the letter-by-letter encipherment of Trithemius—with his own brilliant idea of a literal key, he created the modern concept of polyalphabetic substitution.

It is clear that a key that changes with each message provides more security than one that is used over and over for several messages. The ultimate, of course, is a key that changes with each message. Several men devised an exceedingly clever way to ensure this change: use the message itself as its own key. This is called an "autokey."

The comedy of errors and neglect that constitutes so much of the historiography of cryptology reached a climax of irony when it came to the inventor of the first really acceptable autokey system. It ignored this important contribution and instead named a regressive and elementary cipher for him though he had nothing to do with it. And so strong is the grip of tradition that, despite modern scholarship, the name of Blaise de Vigenere remains firmly attached to what has become the archetypal system of

polyalphabetic substitution and probably the most famous cipher system of all time.

Vigenere was born in the village of Saint-Pourcain, about halfway between Paris and Marseilles, on April 5, 1523. At 24, he entered the service of the Duke of Nevers, to whose house he remained attached the rest of his life, except for periods at court and as a diplomat. In 1549, at 26, he went to Rome on a two-year diplomatic mission.

It was here that he was first thrown into contact with cryptology, and he seems to have steeped himself in it. He read the books of Trithemius, Belaso, and other writers, and the unpublished manuscript of Alberti. He evidently conversed with the experts of the papal curia, for he tells anecdotes that he could have heard only in the shoptalk of these cryptologists. At 47, Vigenere quit the court, turned over his annuity of 1,000 livres a year to the poor of Paris, married the much younger Marie Vare, and devoted himself to his writing. His *Traicte des Chiffres,* which was written in 1585 despite the distraction of a year-old baby daughter, appeared, elegantly rubricated, in 1586, and was reprinted the following year. His autokey system used the plaintext as the key. It provided a priming key. This consisted of a single letter, known to both encipherer and decipherer, with which the decipherer could decipher the first cryptogram letter and so get a start on his, work. With this, he would get the first plaintext letter, then use this as the key to decipher the second cryptogram letter, use that plaintext as the key to decipher the third cryptogram letter, and so on.

| | | | | |
|---|---|---|---|---|
| *key* | DA | UNO | MD | ELETERNE |
| *plain* | au | nom | de | léternel |
| *cipher* | XI | AHG | UP | TMLSHIXT |

The system works well and affords fair guarantees of security; it has been embodied in a number of modern cipher machines.

In spite of Vigenere's clear exposition of his technique, it was entirely forgotten and only entered the stream of cryptology late in the 19th century after it had been reinvented. Writers on cryptology then added insult to injury by degrading Vigenere's system into one much more elementary.

The cipher now universally called the Vigenere employs

only standard alphabets and a short repeating keyword—a system far more susceptible to solution than Vigenere's autokey. Its tableau consists of a modern tabula recta: 26 standard horizontal alphabets, each slid one space to the left of the one above. These are the cipher alphabets. A normal alphabet for the plaintext stands at the top. Another normal alphabet, which merely repeats the initial letters of the horizontal ciphertext alphabets, runs down the left side. This is the key alphabet. Both correspondents must know the keyword. The encipherer repeats this above the plaintext letters until each one has a keyletter. He seeks the plaintext letter in the top alphabet and the keyletter in the side. Then he traces down from the top and in from the side. The ciphertext letter stands at the intersection of the column and the row. The encipherer repeats this process with all the letters of the plaintext. To decipher, the clerk begins with the keyletter, runs in along the ciphertext alphabet until he strikes the cipher letter, then follows the column of letters upward until he emerges at the plaintext letter at the top. For example:

| | |
|---|---|
| *key* | TYPETYPETYPET |
| *plain* | nowisthetimef |
| *cipher* | OMLMLRWIMGBIY |
| *key* | YPETYPETYPET |
| *plain* | orallgoodmen |
| *cipher* | MGEEJVSHBBIG |

Polyalphabetic ciphers were, when used with mixed alphabets and without word divisions, unbreakable to the cryptanalysts of the Renaissance. Why, then, did the nomenclator reign supreme for 300 years? Why did cryptographers not use the polyalphabetic system instead?

Apparently because they disliked its slowness and distrusted its accuracy. Encipherment in a polyalphabetic system, with its need to keep track of which alphabet was in use at every point and to make sure that the ciphertext letter was taken from that alphabet, could not compare in speed with a nomenclator encipherment. The well-informed author of an anonymous 17th-century "Traitte de 1'art de deschiffrer" in the Royal Archives at Brussels stated that chancelleries do not use polyalphabetics because it takes too long to encipher them and because the dropping of a single ciphertext letter garbles the message from that point on. In 1819, William Blair, in a superb encyclopedia article

```
  abcdefghiJklmnopqrstuvwxyz

A ABCDEFGHIJKLMNOPQRSTUVWXYZ
B BCDEFGHIJKLMNOPQRSTUVWXYZA
C CDEFGHIJKLMNOPQRSTUVWXYZAB
D DEFGHIJKLMNOPQRSTUVWXYZABC
E EFGHIJKLMNOPQRSTUVWXYZABCD
P FGHIJKLMNOPQRSTUVWXYZABCDE
Q GHIJKLMNOPQRSTUVWXYZABCDEF
H HIJKLMNOPQBSTUVWXYZABCDEFQ
I IJKLMNOPQHSTUVWXYZABCDEFGH
J JKLMNOPQBSTUVWXYZABCDEFGHI
K KLMNOPQBSTUVWXYZABCDEFGHIJ
L LMNOPQRSTUVWXYZABCDEFGHIJK
M MNOPQRSTUVWXYZABCDEFGHIJKL
N NOPQRSTTUVWXYZABCBEFGHIJKLM
O OPQRSTUVWXYZABCDEFGHIJKLMN
P PQBSTUVWXYZABCDEFGHIJKLMNO
Q QRSTUVWXYZABCDEFGHIJKLMNOP
R BSTUVWXYZABCDEFGHIJKLMNOPQ
S STUVWXYZABCDEFGHIJKLMNOPQB
T TUVWXYZABCDEFGHIJKILMNOPQK
U UVWXYZABCDEFGHIJKLMNOPQRST
V VWXYZABCDEFGHIJKLMNOPQRSTU
W WXYZABCDEFGHIJKLMNOPQBSTUV
X XYZABCDEFGHIJKLMNOPQRSTUVW
Y YZABCDEFGHIJKLMNOPQBSTUVWX
Z ZABCDEFGHIJKLMNOPQBSTUVWXY
```

*The modern Vigenere tableau*

on cryptology, likewise argued that polyalphabetic substitution "requires too much time" and that "by the least mistake in writing is so confounded, that the confederate with his key shall never set it in order again."

One might think that cipher clerks might have corrected such garbles by trial and error, especially in those more leisurely days. But they were not cryptanalysts and may not have known, or have wanted to know, how to make the necessary trials. Serious garbles would thus render the dispatch unreadable until a courier went out and returned with a correction; thus the cipher would have prevented communication instead of safeguarding it.

## 6. The Era of the Black Chambers

REALMONT was under siege. The royal army, under Henry II of Bourbon, Prince of Conde, had invested it at dawn Wednesday, April 19, 1628. But the Huguenots, inside the battlements of the little town in southern France, were putting up a stiff defense. They cannonaded Conde from a tower and contemptuously rejected his demands that they surrender, saying that they would die instead. Conde brought up five big cannon from Albi, a dozen miles away, and on Sunday ranged them in an ominous line facing Realmont.

That same day his soldiers captured an inhabitant of the town who was trying to carry an enciphered message to Huguenot forces outside. None of Conde's men could unriddle it, but during the week the prince learned that it might be solved by the scion of a leading family of Albi who was known to have an interest in ciphers.

Conde sent him the cryptogram. The young man solved it on the spot. It revealed that the Huguenots desperately needed munitions and that, if they were not supplied, they would have to yield. This was news indeed, for despite the destruction of a number of houses by the Catholic batteries, the town was continuing to resist stoutly with no sign of surrender. Conde returned the cryptogram to the inhabitants, and on Sunday, April 30, 1628, though its fortifications were still unbreached and its defenses still apparently adequate for a long siege, Realmont suddenly and unexpectedly capitulated. With this dramatic success began the career of the man who was to become France's first full-time cryptologist: the great Antoine Rossignol.

When word of the incident reached Cardinal Richelieu, the astute and able Gray Eminence of France, he at once attached this useful talent to his suite. Rossignol proved his worth almost immediately. The Catholic armies under Richelieu surrounding the chief Huguenot bastion of La Rochelle intercepted some letters in cipher, which the young codebreaker of Albi read with ease. He told His Eminence that the starving citizens were eagerly awaiting

help that the English had promised to send by sea. When the fleet arrived, the primed guardships and forts so intimidated it that it stood off the port's entrance and made no serious attempt to force a passage. A month later, the city capitulated in full sight of the English vessels—and the great French tradition of expertise in cryptology had been founded.

Rossignol very quickly established himself in the royal service. By 1630, his solutions had made him rich enough to build a small but elegant chateau at Juvisy, 12 miles south of Paris, later surrounding it with a charming informal garden designed by Le Notre, the gardener of Versailles. Here Louis XIII stopped to visit the young crypt-analyst in 1634, 1635 and 1636 on his returns to Paris from Fontainebleau.

In the swashbuckling court of that monarch, and then in the resplendent one of Louis XIV, Rossignol served with an extraordinary facility. The stronghold of Hesdin surrendered a week sooner than it otherwise would have because he solved an enciphered plea for help, and then composed a reply in the same cipher telling the townspeople how futile their hopes were. How many other towns he compelled to surrender, how many diplomatic coups he made possible, how many betrayals he uncovered among the great nobles in those days of shifting allegiances, he never discussed. This reticence caused some at the court to charge that he never actually solved a single cipher, and that the cardinal spread inflated rumors about his abilities to discourage would-be conspirators. But in fact Richelieu was frequently telling his subordinates such things as, "It is necessary to make use, in my opinion, of the letters of the man who has been arrested by the civil authorities at Mezieres, that is to say, have them put into Rossignol's hands to see if there is something important in them." Or, eight years later, in 1642, writing to Messieurs de Noyers and de Chavigny: "I saw, in some extracts, that Rossignol sent me, a truce negotiation of the King of England with the Prince of Orange; I do not think that it can have any effect, but ... it is up to you, gentlemen, to keep your eyes peeled."

Rossignol's work gave him access to some of the greatest secrets of the state and the court, and consequently made him a figure of some prominence in the glittering court of Louis XIV. He appears in some of the major memoirs

of that period. Tallement des Reaux tells some unflattering stories about him and calls him "a poor species of man" in his *Historiettes.* But the Duke of Saint-Simon, whose *Memoires* are a monument of French literature, wrote that Rossignol was "the most skillful decipherer of Europe. . . . No cipher escaped him; there were many which he read right away. This gave him many intimacies with the king, and made him an important man." Rossignol also became the first person to have his biography written solely because of his cryptologic abilities. Charles Perrault, who is better known as the formulator of the Mother Goose tales, included a two-page sketch of Rossignol's life, complete with engraved portrait, in his "Illustrious Men Who Have Appeared in France During This Century," in the company of such as Richelieu. Mazarin regarded his good will as important enough to write a letter of regret in 1658 for some injury done to Rossignol at Paris—and to follow it up two months later with a note to a court official pressing him to do justice to the cryptanalyst "for the insult and violence that has been done him." A more particular sign of importance appears in the largesse that the king showered upon him: 14,000 ecus in 1653, 150,000 livres in 1672, and an annuity, late in his life, of 12,000—to name just some of his payments.*

As he grew old, Rossignol retired to his country home at Juvisy though he reportedly continued to perform his special magic to the end of his life. His last days were brightened by an unmistakable demonstration of royal esteem: the Sun King made a detour in a progress back to Fon-tainebleau to visit him at Juvisy—this in an age when courtiers vied for the privilege of removing the king's pajamas at grand and petit levees each morning! Rossignol died soon after, in December of 1682, only a few days short of his 83rd birthday on January 1.

* One story about Rossignol should be deflated, however. This is that his solutions were made "in a fashion so marvelous to his contemporaries that the device with which a lock is opened when the key has been lost is still called in French a *rossignol."* While the fact of the current usage is true, its implied origin is false. Unfortunately for so charming an etymology, this particular use of the term *rossignol* appears as criminal argot in police documents as early as 1406—almost two centuries before the cryptologist was born. Since the word also means "nightingale," it may be possible that the thieves adopted it as slang for a picklock because its nighttime solos of clicks and rasps were music to their ears.

He had been the cryptologist of France in that incomparable moment when Moliere was her dramatist, Pascal her philosopher, La Fontaine her fabulist, and the supreme autocrat of the world her monarch. Rossignol was, like them, a superlative practitioner of his art at the foremost court of Europe in the very splendor of its golden age.

Black chambers were common during the 1700s, but that of Vienna—the Geheime Kabinets-Kanzlei—was reputed to be the best in all Europe.

It ran with almost unbelievable efficiency. The bags of mail for delivery that morning to the embassies in Vienna were brought to the black chamber each day at 7 a.m. There the letters were opened by melting their seals with a candle. The order of the letters in an envelope was noted and the letters given to a subdirector. He read them and ordered the important parts copied. All the employees could write rapidly, and some knew shorthand. Long letters were dictated to save time, sometimes using four stenographers to a single letter. If a letter was in a language that he did not know, the subdirector gave it to a cabinet employee familiar with it. Two translators were always on hand. All European languages could be read, and when a new one was needed, an official learned it. Armenian, for example, took one cabinet polyglot only a few months to learn, and he was paid the usual 500 florins for his new knowledge. After copying, the letters were replaced in their envelopes in their original order and the envelopes re-sealed, using forged seals to impress the original wax. The letters were returned to the post office by 9:30 a.m.

At 10 a.m., the mail that was passing through this crossroads of the continent arrived and was handled in the same way, though with less hurry because it was in transit. Usually it would be back in the post by 2 p.m., though sometimes it was kept as late as 7 p.m. At 11 a.m., interceptions made by the police for purposes of political surveillance arrived. And at 4 p.m., the couriers brought the letters that the embassies were sending out that day. These were back in the stream of communications by 6:30 p.m. Copied material was handed to the director of the cabinet, who excerpted information of special interest and routed it to the proper agencies, as police, army, or railway administration, and sent the mass of diplomatic material

to the court. All told, the ten-man cabinet handled an average of between 80 and 100 letters a day.

Astonishingly, their nimble fingers hardly ever stuffed letters into the wrong packet, despite the speed with which they worked. In one of the few recorded blunders, an intercepted letter to the Duke of Modena was erroneously re-sealed with the closely similar signet of Parma. When the duke noticed the substitution, he sent it to Parma with the wry note, "Not just me—you too." Both states protested, but the Viennese greeted them with a blank stare, a shrug, and a bland profession of ignorance. Despite this, the

j existence of the black chamber was well known to the various delegates to the Austrian court, and was even tacitly acknowledged by the Austrians. When the British

'ambassador complained humorously that he was getting copies instead of his original correspondence, the chancellor replied coolly, "How clumsy these people are!"

Enciphered correspondence was subjected to the usual cryptanalytic sweating process. The Viennese enjoyed remarkable success in this work. The French ambassador, who was apprised of its successes from papers sold him by a masked man on a bridge, remarked in astonishment that "our ciphers of 1200 [groups] hold out only a little while against the ability of the Austrian decipherers." He added that though he suggested new ways of ciphering and continual changes of ciphers, "I still find myself without secure means for the secrets I have to transmit to Constantinople, Stockholm, and St. Petersburg."

The Viennese owed at least some of their success to their progressive personnel policies. Except in emergencies, the cryptanalysts worked one week and took off one week— apparently to keep them from cracking under the intense mental strain of the work. Though the pay was not high, substantial bonuses were given for solutions. For example, bonuses totalling 3,730 florins were disbursed between March 1, 1780, and March 31, 1781, for the solution of 15 important keys. Perhaps the most important incentive was the prestige accorded to the cryptanalysts by direct royal recognition of their value. Karl VI personally handed the cryptanalysts their bonuses and thanked them for their work. Empress Maria Theresa conferred frequently with the officials of the black chamber about the cipher service and the cryptanalytic ability of other countries; that remarkable woman demonstrated her grasp of the principles

1

involved by inquiring whether any of her ambassadors had corresponded too much in a single nomenclator and ought to be given a new key. The cryptanalysts sometimes even got paid for not solving a cipher: if a key was stolen from an embassy, the codebreakers would get a kind of unemployment compensation because they had no opportunity to win their bonus. In 1833, for example, the cabinet got three fifths of the solution bonus when the key of the French envoy was stealthily removed, copied, and replaced in a cupboard in the bedroom of the secretary of the French legation within a single night.

A good glimpse into the achievements of the Geheime Kabinets-Kanzlei is afforded by the letters of one of its best directors, Baron Ignaz de Koch, who served from 1749 to 1763 with the cover-title of secretary to Maria Theresa. On September 4, 1751, he sent to the Austrian ambassador in France some cryptanalyzed correspondence which "makes one see more and more the main principles that direct the cabinet in France." Two weeks later, in referring to some other cryptanalyses, he wrote, "This is the eighteenth cipher that we have got through during the course of the year; ... we are regarded, unhappily, as being too able in this art, and this thought makes the courts that fear that we can engross their correspondence change their keys at every instant, so to speak, each time sending ones more difficult and more laborious to decipher." Among letters solved during its existence were those of Napoleon, Talleyrand, and a host of lesser diplomats. These solutions were often made the basis of Austrian strategy.

England, too, had its black chamber. It began with the cryptanalytic endeavors of John Wallis, the greatest English mathematician before Newton. After his death, it descended through his grandson to reach, on May 14, 1716, Edward Willes, a 22-year-old minister at Oriel College, Oxford.

Willes embarked at once upon a career unique in the annals of cryptology and the church. He not only managed to reconcile his religious calling with an activity once condemned by churchly authorities, but also went on to become the only man in history to use cryptanalytic talents to procure ecclesiastical rewards. Within two years, he had been named rector of Barton, Bedfordshire, for solving more than 300 pages of cipher that exposed Sweden's

attempt to foment an uprising in England. He virtually guaranteed his future when he testified before the House of Lords in 1723. Here, Francis Atterbury, Bishop of Rochester, was being tried by his peers for attempting to set a pretender on the English throne.

The pretender's cause exhorted the allegiance of many in England, and the nation's attention focused on Atterbury's trial. Most of the facts about the alleged conspiracy had come from his intercepted correspondence, and the most inculpatory evidence had been extracted from the portions in cipher by Willes and by Anthony Corbiere, a former foreign service official in his mid-thirties who had also been appointed a Decypherer in 1719. The Lords "thought it proper to call the Decypherers before them, in order to their being satisfied of the Truth of the Decyphering." To demonstrate this, Willes and Corbiere deposed,

> That several Letters, written in this Cypher, had been decyphered by them separately, one being many Miles distant in the Country, and the other in Town; and yet their Decyphering agreed;
>
> That Facts, unknown to them and the Government at the Time of their Decyphering, had been verified in every Circumstance by subsequent Discoveries; as,
>
> particularly, that of *H------'s* Ship coming in Ballast
>
> to fetch *O*------- to *England* which had been so de-cyphered by them Two Months before the Government had the least Notice of *Halstead's* having left *England;*
>
> That a Supplement of this Cypher, having been found among *Dennis Kelly's* Papers the latter End of *July,* agreed with the Key they had formed of that Cypher the *April* before;
>
> That the Decyphering of the Letters signed *Jones lllington* and 1378, being afterwards applied by them to others written in the same Cypher, did immediately make pertinent Sense, and such as had an evident Connexion and Coherence with the Parts of those Letters that were out of Cypher, though the Words in Cypher were repeated in different Paragraphs, and differently combined.

The two Decypherers appeared before the Lords on several occasions to swear to their solutions. Attenbury twice

objected and was twice overruled. But on May 7, as Willes was testifying to the cryptanalysis of the three most incriminatory letters of all, and the bishop felt the noose tightening around him, he persisted in questioning Willes on the validity of the reading though the House had supported Willes' refusal to answer. He raised such a commotion that he and his counsel were ordered to withdraw, and the Lords voted upon the proposition, "that it is the Opinion of this House that it is not consistent with the public Safety, to ask the Decypherers any Questions, which may tend to discover the Art or Mystery of Decyphering." It was resolved in the affirmative, the solutions were accepted, and Atterbury, largely on this evidence, was found guilty, deprived of office, and banished from the realm.

Willes, on the other hand, became Canon of Westminster the next year. His salary more than doubled to £500. He succeeded to ever more important posts every four or six years thereafter, and finally, in 1742, when the oldest of his three sons, Edward, Jr., obtained a patent as a Decypherer, he was created Bishop of St. David's, being translated the next year to the more prestigious see of Bath and Wells. The bishop and his son shared the substantial salary of £1,000 a year. In 1752, he brought another son, William, into the business at an eventual £200, and six years later a third son, Francis, who for some reason served without pay.

Bishop Willes died in 1773 and was buried in Westminster Abbey. His sons Edward, Jr., and Francis inherited a large share of his fortune and landed property and, living as wealthy squires at Barton and Hampstead, continued their cryptanalytic work. Their brother William had retired in 1794, but his three sons, Edward, William, and Francis Willes joined the Decyphering Branch in the 1790s.

Though the Willes family dominated the cryptanalytic branch, others worked in it. Corbiere was paid through such sinecures as his appointment as naval officer at Jamaica, though he never stirred from England, and as Commissioner of Wines Licenses, which sounds like the cushiest of posts. He rose to Under Secretary of the Post Office but continued his cryptanalytic work, which ended after 24 years only with his death in 1743, when he was receiving £800. The other cryptanalysts at various times were James Rivers, Frederick Ashfield, John Lampe,

f George Neubourg, John Bode, Jr., one Scholing, and a Boelstring.

\ These men received their foreign interceptions from the :' Secret Office and their domestic ones from the Private - Office, both subdivisions of the Post Office. The Secret Office was quartered in three rooms adjoining the Foreign Office and entered privately from Abchurch Lane. Fire and candles burned constantly in one room; the staff lodged in the others. It included men who made their life's work the specialty of unsealing diplomatic packets with such, deftness that they could be resealed without evidence of tampering; one such opener was J. E. Bode, father of John Bode, Jr. He regularly spent three hours on the dispatches of the King of Prussia, opening them and then re-sealing them with special wax and carefully counterfeited seals. Perhaps surprisingly in a bastion of human rights, its interceptions enjoyed full legality. The statute of 1657 that established the postal service declared outright that the mails were the best means of discovering dangerous and wicked designs against the commonwealth. Leases of 1660 and 1663, confirmed by the Post Office Act of 1711, permitted government officials to open mail under warrants that they themselves issued. They sidestepped this bothersome procedure by promulgating all-inclusive general warrants.* The Secret Office sent interceptions en clair to the king and those in cipher to the cryptanalysts.

They were known collectively as the Decyphering Branch. Unlike the Secret Office, the branch had no specific location. Its tiny staff of experts worked largely at home, receiving their material by special messenger. Nor had it any formal organization, the senior Decypherer being merely first among equals. More secret than the Secret Office, the branch's funds came from secret-service money issued to the Secretary of the Post Office from Parliament's surplus revenue. Security was tight—in all of England probably only 30 people knew what diplomatic correspondence was being read at any given moment. Nevertheless, most men of affairs were aware of the practice of opening

*This activity forms the legal precedent for the modern tapping of telephones, at least in Britain. Significantly, however, the source of the power to intercept communications has never been determined. The Crown simply exercised it and, despite occasional debate, has continued to do so, presumably with the tacit approval of the public as necessary for the safety of the state.

private letters, and they often enciphered their correspondence or entrusted it to private messengers when secrecy was essential.

After the Elector of Hanover succeeded to the English throne as George I in 1714, retaining the rule of the German state, the Decyphering Branch collaborated with the black chamber maintained at Nienburg by the Hanoverian government. Cryptanalysts Bode, Lampe, and Neubourg had even been imported from there—an ironic development in view of a refusal of Wallis to divulge his technique to Hanover a few years earlier. Mail opening became habitual. George and his successors took a constant personal interest in the work, often encouraging talent with royal bounty. Correspondence was closely watched for cribs that were passed to the Decyphering Branch.

During the 1700s, the branch's output averaged two or three dispatches a week, and sometimes one a day. Its cryptanalysts solved the dispatches of France, Austria, Saxony and other German states, Poland, Spain, Portugal, Holland, Denmark, Sweden, Sardinia, Naples and other Italian states, Greece, Turkey, Russia, and, later, the United States. The record of French interceptions covers two centuries and comprises five volumes of intercepts totaling 2,020 pages plus three volumes of keys. Perhaps more typical is the Spanish dossier—three volumes of intercepts from 1719 to 1839 totaling 872 pages. Not all of the messages were solved at the time of their interception. Many were held either until enough had accumulated for a successful attack or until a need arose for their solution.

The solutions were read by the king and a few of the top ministers. They warned the government of the intrigues of foreign rulers and ambassadors and of impending war. An intercepted message between the Spanish ambassadors in London and Paris clearly suggested that Spain had allied herself with France against England in the Seven Years' War. It was read at the British cabinet meeting of October 2, 1761. The Great Commoner, William Pitt the Elder, cited it as support for his proposal that England take the initiative, declare war before Spain did, and capture the fleet of treasure ships then transporting gold to Spain from her American possessions. His counsel was rejected, and he resigned. The war came anyway—after the immense cargo of bullion had been unloaded at Cadiz.

In the 1840's, political gales blew down a great deal of

the remaining absolutism and the totalitarian agencies that propped it up. Europe's new birth of freedom tolerated no government opening of mail. In England, a tremendous public and parliamentary outcry over the surreptitious opening of letters forced the government to discontinue the interception of diplomatic correspondence in June of 1844. That October the government dissolved the Decyphering Branch, pensioning off Willes and Lovell. In Austria, the Geheime Kabinets-Kanzlei closed its doors in 1848. In France, the Cabinet Noir, which had been withering ever since the Revolution, passed away as well in that convulsive year. And in that same decade, the same vast social forces that ended the era of the black chambers simultaneously fostered an invention that transformed cryptography.

## 7. The Contribution of the Dilettantes

THE TELEGRAPH made cryptography what it is today. Samuel F. B. Morse sent "What hath God wrought!" in 1844. The next year his lawyer and promotional agent, Francis O. J. Smith, published a commercial code entitled *The Secret Corresponding Vocabulary; Adapted for Use to Morse's Electro-Magnetic Telegraph,* in whose preface he declared that "secrecy in correspondence, is far the most important consideration." This was provided by a super-encipherment.

As the most exciting invention of the first half of the century, the telegraph stirred as much interest in its day as Sputnik did in its. The great and widely felt need for secrecy awakened the latent interest in ciphers that so many people seem to have, and kindled a new interest in many others. Dozens of persons attempted to dream up their own unbreakable ciphers. Their contributions enriched it with dozens of new cipher systems.

As businessmen and the public used the telegraph more and more, they found that their fears about lack of privacy were exaggerated. The clerks dealt impersonally with the messages. The telegraph companies respected their confidentiality. And commercial codes like Smith's, which replaced words and phrases by single codewords or code-

numbers to cut telegraph tolls, afforded sufficient security for most business transactions by simply precluding an at-sight comprehension of the meaning. The brokers and traders soon realized that the main advantage of these codes was their economy.

Government ministries used the telegraph, too. At first they must have encoded with their nomenclators. But although secrecy was paramount for them, they liked the telegraphic economy of a large code—especially as they telegraphed more and more. So when the time arrived to compile a new nomenclator, they abandoned that form, copied the commercial form, and produced a full-fledged code. The nomenclators had had their 1,- or 2,000 code-numbers in mixed order, but the war and foreign ministries balked at the expense of drawing up a 50,000-entry code in two parts, and they had no professional cryptanalysts to warn them of the danger of the one-part format. They relied for security upon small editions, big safes, extensive lexicon (large codes are harder to break than small ones, other things being equal), and superencipherment, retaining codenumbers to facilitate this instead of switching to codewords. This evolution was essentially complete by the 1860s. The large, one-part code had replaced the small, two-part nomenclator in high-level military and diplomatic cryptography.

Meanwhile, the telegraph, author of this development, was creating something new in war—signal communications, or voluminous command and reconnaissance messages. Of course such messages had existed before, with torches, pigeons, and couriers, but in so rarefied a form that they were not even called "signal communications." The telegraph enabled commanders, for the first time in history, to exert instantaneous and continuous control over great masses of men spread over large areas.

These tactical messages required protection: telegraph wires could be tapped. Neither the old nomenclator nor the new code would do. They were too easy to capture in combat, too hard to reissue quickly and frequently to the numerous and widespread telegraph posts. Signal officers turned away from them. They looked instead to that neglected child of cryptography, the cipher. Ciphers could be printed cheaply on a single sheet of paper and distributed with ease. Secrecy was based upon variable keys, so capture of the general system and even of one of the

keys would not compromise all an army's secret messages. Solutions would be prevented by rapid key changes. Ciphers were ideal for battle-zone messages, and the first of the modern wars, the American Civil War, used them for just that. Thus was born a new genre in cryptography: the field cipher.

The first one was waiting in the wings. This was poly-alphabetic substitution, in the form of the straight-alphabet Vigenere with short repeating keyword. The old objections to its use, which boiled down to the impossibility of correcting a garbled dispatch quickly enough, vanished with the telegraph. It fulfilled the requirements of noncom-promisability of the general system and of ease of key changes. Moreover, it had the reputation of being unbreakable—which, if its cryptograms were not divided into words, it largely was. The military adopted it at once.

Then, in 1863, a retired Prussian infantry major discovered the general solution for the periodic polyalpha-betic substitution. At one stroke he demolished the only impregnable structure in cryptography. Signal officers, compelled to provide secure communications, hunted frantically for new field ciphers. They found many good ideas in the writings of the dilettante cryptographers who had proposed ciphers for the protection of private messages. Soon some of these systems were serving in the various armies of Europe and the Americas. More ideas came from army officers who had studied cryptography in the courses in signal communication that the national military academies, such as St. Cyr, had added in the mid-1800s. Inevitably, cryptanalysts—who were either amateurs or soldiers with a professional interest, for full professionals there were none—replied with new techniques for breaking the new ciphers. From the slow crawl of nomenclator days, when the introduction of a special group meaning *Disregard the preceding group* would constitute a remarkable technical advance, the race between offense and defense in cryptology acclerated to its modern pace.

The history of cryptology from the decade that saw both the death of the black chambers and the birth of the telegraph to World War I is thus a story of internal development. Without Rossignols or Willeses, and without major wars or diplomatic struggles, cryptology could not influence world events, and, except for one or two unusual cases, it did not. The telegraph launched this evolution

of cryptology. It broke the monopoly of the nomenclator. The nomenclator had reigned for 450 years as a general, all-purpose system, but it could not meet the new requirements either of high-level diplomatic or military communications or of low-level signal communications, which the telegraph had engendered. Each called for its own kind of cryptosystem, a specialized one. Signal officers ranked these systems in a hierarchy, rising from the simple and flexible and easily solved to the extensive and hard to solve. The telegraph thus stimulated the invention of many new ciphers and, by reaction, many new methods of crypt-analysis, and compelled their arrangement in a scale of complexity.

Many of these ciphers and techniques have become classic and are in use today. Moreover, cryptography still functions through a hierarchy and employs a multitude of special systems. The telegraph thereby furnished cryptography with the structure and the content that it still has. It made it what it is today.

All these things have antecedents, and just as the telegraph itself did, so were there precursors of the cryptographic systems that it engendered.

One cipher system invented before the telegraph was so far ahead of its time, and so much in the spirit of the later inventions, that it deserves to be classed with them. Indeed, it deserves the front rank among them, for this system was beyond doubt the most remarkable of all. So well conceived was it that today, more than a century and a half of rapid technological progress after its invention, it remains in active use.

But then it was invented by a remarkable man, a well-known writer, agriculturalist, bibliophile, architect, diplomat, gadgeteer, and statesman named Thomas Jefferson. He called it his "wheel cypher," and it seems likely that he invented it either during 1790 to 1793 or during 1797 to 1800.

> Turn a cylinder of white wood of about 2. Inches diameter & 6. or 8. I. long, bore through it's center a hole sufficient to receive an iron spindle or axis of *Vs* or $^{1}A$ I. diam. divide the periphery into 26. equal parts (for the 26. letters of the alphabet) and, with a sharp point, draw parallel lines through all the points

of division from one end to the other of the cylinder, & trace those lines with ink to make them plain, then cut the cylinder crosswise into pieces of about *V6* of an inch thick, they will resemble back-gammon men with plane sides, number each of them, as they are cut off, on one side, that they may be arrangeable in any order you please, on the periphery of each, and between the black lines, put all the letters of the alphabet, not in their established order, but jumbled & without order, so that no two shall be alike, now string them in their numerical order on an iron axis, one end of which has a head, and the other a nut and screw; the use of which is to hold them firm in any given position when you chuse it. they are now ready for use, your correspondent having a similar cylinder, similarly arranged.

Suppose I have to cypher this phrase. "Your favor of the 22d is received."

I turn the 1" wheel till the letter y. presents itself

I turn the *2* &* place it's . . o. by the side of the y. of the !•' wheel

I turn the 3d & place it's . . u. by the side of the o. of the 2a

4th.....r. by the side of the u. of the 3d

5">.....f. by the side of the r. of the 4th

6th.....a. by the side of the f. of the 5th

and so on till I have got all the words of the phrase arranged in one line, fix them with the screw, you will observe that the cylinder then presents 25. other lines of letters, not in any regular series, but jumbled, & without order or meaning, copy any one of them in the letter to your correspondent, when he receives it, he takes his cylinder and arranges the wheels so as to present the same jumbled letters in the same order in one line, he then fixes them with his screw, and examines the other 25. lines and finds one of them presenting him these letters: "yourfavorofthe 22isreceive d." which he writes down, as the others will be jumbled & have no meaning, he cannot mistake the true one intended, so proceed with every other portion of the letter, numbers had better be represented by letters with dots over them; as for instance by the 6. vowels & 4. liquids, because if the periphery were divided into 36. instead of 26. lines for the numerical, as well as alphabetical characters,

it would increase the trouble of *finding the* letters on the wheels.

When the cylinder of wheels is fixed, with the jumbled alphabets on their peripheries, by only changing the order of the wheels in the cylinder, an immense variety of different cyphers may be produced for different correspondents, for whatever be the number of wheels, if you take all the natural numbers from unit to that inclusive, & multiply them successively into one another, their product will be the number of different combinations of which the wheels are susceptible, and consequently of the different cyphers they may form for different correspondents, entirely unintelligible to each other. . . .

Jefferson went on to say that if the cylinder be six inches long ("which probably will be a convenient length, as it may be spanned between the middle finger & thumb of the left hand, while in use") the number of wheels would total 36, and the number of ways in which they can be strung on the spindle to form different ciphers for different correspondents would come to 36 factorial, or 1 X 2 X 3 X ... X 35 X 36, which Jefferson calculated almost exactly as "372 with 39 cyphers [zeros] added to it." In fact, 36 factorial is 371,993,326,789,901,217,467,999,448,150,835, 200,000,000.

Had the President recommended his own system to Secretary of State James Madison, he would have endowed his country with a method of secret communication that would almost certainly have withstood any cryptanalytic attack of those days. Instead he appears to have filed and forgotten it. It was not rediscovered among his papers in the Library of Congress until 1922, coincidentally the year the U.S. Army adopted an almost identical device that had been independently invented. Later, other branches of the American government used the Jefferson system, generally slightly modified, and it often defeated the best efforts of the 20th-century cryptanalysts who tried to break it down! To this day the Navy uses it. This is a remarkable longevity. So important is his system that it confers upon Jefferson the title of Father of American Cryptography.

[Codebreakers 117.jpg]

Charles Wheatstone had a remarkably fertile mind. He constructed an electric telegraph before Morse did, invented

the concertina, improved the dynamo, studied underwater telegraphy, produced some of the first stereoscopic drawings, published half a dozen papers on acoustics, discussed phonetics and hypothetical speaking machines in print, conducted numerous electrical experiments, and popularized a method for the extremely accurate measurement of electrical resistance now in frequent use and called the "Wheatstone bridge." His work was highly enough regarded for him to be elected a fellow of the Royal Society and to be knighted. He was nominally professor of experimental

philosophy at King's College, London, but was so excessively shy that he hardly ever actually lectured.

Another of his inventions was a cipher for secrecy in telegraphy, which, however, carries the name of his friend Lyon Playfair, first Baron Playfair of St. Andrews. A scientist and public figure of Victorian England, Playfair was at one time or another deputy speaker of the House of Commons, postmaster general, and president of the British Association for the Advancement of Science.

Playfair demonstrated what he called "Wheatstone's newly-discovered symmetrical cipher" at a dinner in January, 1854, given by the president of the governing council, Lord Granville. One of the guests was Queen Victoria's husband, Prince Albert; another was the Home Secretary and future Prime Minister, Lord Palmerston. Playfair explained the system to him, and, while in Dublin a few days later, received two short letters in the cipher from Palmerston and Granville, showing that both had readily mastered it.

The cipher is the first literal one in cryptologic history to be digraphic*—that is, to encipher two letters so that the result depends upon both together. Wheatstone recognized that the cipher would work as well with a rectangle as with a square, but it soon petrified into the latter form. Playfair thus constructed a square based on PALMERS-TON, with the remaining letters of the alphabet following, to illustrate the cipher at Granville's dinner:

PALME R S T O N B C D F G H IJ K Q U V W X Y Z

To encipher, the plaintext is divided into pairs. Double letters occurring together in a pair must be separated with an *x,* so that *balloon* would be enciphered as *ba Ix lo on; i* and / are regarded as identical, so that *adjacent* will be enciphered as if it were *adjiacent.* Now the letters of each pair may stand in only three relationships to one another within the square: the two may appear in the same row, in the same column, or in neither. Letters that fall in the

*An earlier author's digraphic table used not letters but signs.

same row are each replaced by the letter to its right. Thus, *am* = LE, *hi* = IK, *os* = NT. Each row is considered cyclical, so that the letter to the right of the last letter in a row is the first letter at the left of that row. Thus, *le* = MP, *ui* — HK. Letters that appear in the same column are each replaced by the letter beneath it; the cyclical provision holds. Thus, *ac* = sj (or si, as the encipherer wishes); *of* = FQ, *wi* — AW, *br* = HB.

If the plaintext letters appear in neither the same row nor the same column, each is replaced by the letter that lies in it's own row and stands in the column occupied by the other plaintext letter. For example, to encipher *sq,* the encipherer first locates them in the square. Then he runs across the row of the first plaintext letter *(s)* until he meets the column in which the second plaintext letter *(q)* stands:

. M .

R *S* T O N

. . . F .

. • • *Q* •

. Y .

The letter at the junction of row and column (o) becomes the first cipher letter. Then the encipherer traces across the row of the second plaintext letter *(q)* until he intersects the column in which the first plaintext letter stands:

. A ...

5 ...

. C . . .

H IJ K *Q* U

. W .

The letter at the intersection (i) becomes the second cipher letter. Thus *sq* = 01. Other encipherments are *af* = MC, *at* = LS, *ed* — LG. The letter in the row of the first plaintext letter is always taken first to preserve the order of the letters, so that *cl* — DA and not AD, which would stand for *le,* and *ve* = ZA.

Decipherment in this is precisely the same as encipher-ment: if *ow* = SY, then *sy* — ow. In the other two cases, the plaintext letters are found to the left or above the ciphertext letters. Thus, using the same square, a ciphertext reduces as follows:

MT TB BN ES WH TL MP TA LN NL NV

lo rd gr an vi Ix le si et te rz

The *z* at the end is a null to complete the final digraph.

Wheatstone and Playfair explained the cipher to the Under Secretary of the Foreign Office, no doubt pointing out its chief advantage—that two plaintext pairs that have a letter in common may not display the slightest resemblance in ciphertext, as *le* and *te* above were enciphered to MP and NL. Further, once mastered, it rolls along with remarkable ease and rapidity. When the Under Secretary protested that the system was too complicated, Wheatstone volunteered to show that three out of four boys from the nearest elementary school could be taught it in 15 minutes. The Under Secretary put him off. "That is very possible," he said, "but you could never teach it to attaches."

Playfair, reasoning that this reflected more on the diplomats than on the cipher, remained enthusiastic about it. There were good grounds for enthusiasm. In the first place, the cipher's being digraphic obliterates the single-letter characteristics—*e,* for example, is no longer identifiable as an entity. This undercuts the usual monographic methods of frequency analysis. Secondly, encipherment by digraphs halves the number of elements available for frequency analysis. A 100-letter text will have only 50 cipher digraphs. In the third place, and most important, the number of digraphs is far greater than the number of single letters, and consequently the linguistic characteristics spread over many more elements and so have much less opportunity to individualize themselves. There are 26 letters but 676 digraphs; the two most frequent English letters, *e* and *t,* average frequencies of 12 and 9 per cent; the two most frequent English digraphs, *th* and *he,* reach only *3¹/** and *2V2* per cent. In other words, not only are there more units to choose among, the units are less sharply differentiated. The difficulties are doubly doubled.

These properties elevated the cipher above most of its contemporaries purely on cryptographic considerations; it was, properly, regarded as unbreakable. Its many practical excellences—no tables or apparatus required, a keyword that could easily be remembered and changed, great simplicity of operation—commended it as a field cipher. Play-fair suggested that it be used as just that in the impending

Crimean War when he brought it up at the dinner with Prince Albert. No evidence exists that it was used then, but there are reports that it served in the Boer War. Britain's War Office apparently kept it secret because it had adopted the cipher as the British Army's field system. Playfair's unselfish proselytizing for his friend's system unwittingly cheated Wheatstone of his cryptographic heritage; though Playfair never claimed the invention as his own, it came to be known in the War Office as Playfair's Cipher, and his name has stuck to it to this day.

Five years later, an American who at the time was working for a stove and foundry firm glanced briefly at cryp-tology and produced a single short piece of work. It opened important new vistas into untrodden lands—and then sank immediately into a cryptologic obscurity.

The inventor was Pliny Earle Chase, then 39, who, after entering Harvard as a prodigy at 15, taught in Philadelphia for seven years until his health forced him into less tiring work in business. In 1861 he resumed teaching, becoming professor of natural science and then professor of philosophy and logic at Haverford College near Philadelphia. He was an absorbing lecturer, particularly in astronomy, and he collaborated on an arithmetic textbook with Horace Mann. But perhaps his most notable accomplishment was his writing more than 250 articles for scholarly magazines. Among them was the one that he penned in 1859 which covered barely three pages in the new *Mathematical Monthly,* but which constitutes the first published description of fractionating, or tomographic, cipher systems.

The basis of these ciphers stretches back across the millennia to Polybius, the Greek historian of the second century B.C. who distributed the alphabet in what is even today sometimes called a "Polybius square," but more often a "checkerboard." Numbers at the side and top indicate the row and the column of a given letter. Similar systems have cropped up throughout cryptography. Some replace the alphabet by three symbols in groups of three *(a* = 111, *b* — 112, *c* — 113, *d* — 121, etc.), some by two in groups of five (a = 00000, *b* = 00001, c = 00010, etc.). But no one seems to have seen the symbols as manipulable entities instead of just as an unalterable part of the whole.

Until Chase. He severed the coordinates from one another and subjected the resulting fractions to various crypto-

graphic treatments. He began with a checkerboard filled out to ten columns with Greek letters:

---

6

Chase wrote his coordinates vertically, so that his sample plaintext, *Philip,* appeared like this:

133131 959899

He then multiplied the lower line by 9, obtaining the result:

133131 8639091

This he restored to literal form by resubstituting back in his checkerboard, 8 (by itself) = L, j, or T, then 16 = N, 33 = s, 39 = i, and so on, with the final ciphertext

**LNSl4>IX.**

Chase proposed other means of transforming the bottom row, such as adding a repeating key or giving the logarithm of the row, and pointed out that even more intricate processes might be used. "But the simpler cypher, provided it is effectual, is the better," he wisely concludes. The Chase systems grant a fairly hermetic security; they are, besides, relatively simple to operate. Yet cryptologic history shows no one ever having used them, even though they are far superior to many systems that have seen service.

Of the man who did explode the bomb that gouged new channels for cryptology, little more is known than the bare outline provided by his service record. This is complete if not detailed, for Friedrich W. Kasiski spent his entire professional career as an officer in East Prussia's 33rd Infantry Regiment. Born November 29, 1805, in what was then Schlochau, West Prussia, and is now Czluchow, Poland, he enlisted in the regiment at 17. He won his commission as a second lieutenant three years later, in 1825—and did not budge out of that rank for 14 years. But he remained a

first lieutenant only three years before he was promoted to captain and company commander, a post he held for nine years. He retired in 1852 with the rank of major, and though he served from 1860 to 1868 as the commander of a National Guard-like battalion, he found sufficient leisure to devote some to cryptology, for in 1863 his short but epochal book was published in Berlin by the respected house of Mittler & Sohn.

Three quarters of *Die Geheimschriften und die Dechif-frir-kunst* concentrates on answering the problem that had vexed cryptanalysts for more than 300 years: how to achieve a general solution for polyalphabetic ciphers with repeating keywords. (One chapter zeroes in on "The Decipherment of French Writing"—a rather ominous portent in a book dedicated to the Count Albrecht von Roon, the Prussian minister of war who molded the army that humbled France only seven years later.) The polyalphabetic solution opened the doors to the cryptology of today. But the 95-page volume seems to have stirred almost no comment at the time. Kasiski himself lost interest in cryptology. He became an avid amateur anthropologist, joining the Natural Science Society of Danzig, unearthing prehistoric graves, and reporting on his work to learned journals. (One of his scholarly articles was cited in the *Encyclopaedia Britannica.)* Kasiski died on May 22, 1881, almost certainly without realizing that he had wrought a revolution in cryptology.

That revolution began when Kasiski shrewdly noted a phenomenon: the conjunction of a repeated portion of the key with a repetition in the plaintext produces a repetition in the ciphertext:

*key* RTJNRTJNRUNRUNRTJNRUNRUNRTJNRtJNRUN

*plaintext* tobeornot tobethatisthequestion *ciphertext* KIO v i E E i o K I o v NUB N v J N u VKHVMQZ I A

Each time that the key RUNR engages the repeated plaintext *to be,* the repeated ciphertext tetragraph KIOV results. Like causes produce like effects. Similarly, when the repeated key-fragment UN operates upon the repeated *th's,* the ciphertext registers repeated NU'S.

Clearly, the keyword must repeat one or more times for a given part of it to encipher two identical bits of plaintext several letters distant from one another. The number of letters between the two resultant ciphertext repetitions will

itwv_uu inc numoer or times that the keyword has repeated. The count of the interval "between" the two repetitions actually includes repeated letters. Thus the interval between the first KIOV and the second is 9, figured like this: 5 letters not repeated and 4 that are. This interval of nine results from the fact that the keyword has three letters and has repeated three times. These repetitions betray the movements of the keyword beneath the surface of the cryptogram just as the ducking of a fishing cork tells of a nibble. Kasiski said to locate all repetitions in the cryptogram and then to "calculate the distance separating the repetitions from one another. . . . and endeavor to break up this number into its factors. . . . The factor most frequently found indicates the number of letters in the key." For example, an interval of 60 will show factors of 2 X 2 X 3 X 5. If the factors of 2 X 3 occur in most of the calculations, the keyword probably has six letters in it. Now, knowledge of how many letters are in the keyword tells how many alphabets were used in the polyalphabetic encipher-ment. This information permits the cryptanalyst to sort the letters of the cryptogram so that all those enciphered with the first keyletter are brought together in one group, all those enciphered with the second keyletter in another group and so forth. Since all of the, say, *e's* in the first group were converted under the influence of a single key-letter to the same ciphertext, all of the *a's* to one ciphertext letter, and so on, each of these collections of letters constitutes a monoalphabetic substitution cipher and so can be solved like one. When he reassembles these, he will have the plaintext to an "unbreakable" cipher.

It was France, however, that published one of cryptol-ogy's greatest books. *La Cryptographic militaire* first appeared as two installments in the *Journal des Sciences militaires* in January and February of 1883, being reissued later that year as a paperback book by the journal's publisher. It is the most concise book on cryptology ever written. Its author had the instinct for the cryptographic jugular, and he compressed into 64 pages virtually the entire known field of cryptology, including polyalphabetics with mixed alphabets, enciphered code, and cipher devices. The book is also one of the most scholarly on cryptology. Its footnotes cite most classical and many modern sources; comments such as "This is not the only historical or

bibliographic error for which the Austrian writer must be reproached" show how carefully the author has studied those sources.

Its author was born Jean-Guillaume-Hubert-Victor-Frangois-Alexandre-Auguste Kerckhoffs von Nieuwenhof on January 19, 1835, at Nuth, Holland. After getting degrees in letters and in science from the University of Liege, he was hired in 1863 as an instructor in modern languages at the high school at Melun, a large town 25 miles southeast of Paris. The next year he married a girl from the area and in 1865, when he was 30, they had their only child, a daughter, Pauline. He stayed at Melun for 10 years, teaching English and German.

By that time he had shortened his name to Auguste Kerckhoffs. Bearded, dignified, slow of speech, Kerckhoffs, despite an inability to maintain discipline in his classes and some eccentricities of character, was a "learned, zealous, capable" teacher who awoke his students' interest in their work; his superiors said "his students like him and work with success." Afterward, he worked as a private instructor in Paris.

His busiest years followed the publication of *La Cryptographic militaire.* A new international language called Vola-piik ("World-Speak") had been invented by a German priest. About 1885, it caught on in France and flashed with express-train speed all over the country, not only among intellectuals but among all classes; it was even heard in the streets. From France it radiated throughout the world. The most active propagandist of Volapiik was Auguste Kerckhoffs, who, at the second Volapiik congress in Munich in 1887, was acclaimed director ("Dilekel," in Volapiik) of the International Academy of Volapiik. But at the third congress, held at Paris in May of 1889, with Kerckhoffs presiding, critical tensions within the movement mounted and finally broke it apart.

Kerckhoffs was crushed by the collapse of an international dream that had seemed so needful and so certain. He created nothing else and, on August 9, 1903, died while on vacation in Switzerland.

But his cryptologic ideas still nourish. For Kerckhoffs sought answers to the problems thrust upon cryptology by new conditions. "It is necessary to distinguish carefully between a system of encipherment envisioned for a momentary exchange of letters between several isolated people

and a method of cryptography intended to govern the correspondence between different army chiefs for an unlimited time," he wrote. In that one sentence, Kerckhoffs differentiates pre-telegraphy military communications from post-. The sentence is pregnant with most of the requirements that have come to be demanded of systems of military cryptography, requirements such as simplicity, reliability, rapidity, and so on. This clear recognition of the new order constitutes Kerckhoffs' first great contribution to cryptology.

The second was to reaffirm in a modern context the principle that only cryptanalysts can know the security of a cipher system. It is the form of judgment which is still used.

From these two fundamental principles for selecting usable field ciphers, Kerckhoffs deduced six specific requirements: (1) the system should be, if not theoretically unbreakable, unbreakable in practice; (2) compromise of the system should not inconvenience the correspondents; (3) the key should be rememberable without notes and should be easily changeable; (4) the cryptograms should be transmissible by telegraph; (5) the apparatus or documents should be portable and operable by a single person; (6) the system should be easy, neither requiring knowledge of a long list of rules nor involving mental strain.

These requirements still comprise the ideal which military ciphers aim at. They have been rephrased, and qualities that lie implicit have -been made explicit. But any modern cryptographer would be very happy if any cipher fulfilled all six.

Of course, it has never been possible to do that. There appears to be a certain incompatibility among them that makes it impossible to institute all of them at once. The requirement that is usually sacrificed is the first. Kerckhoffs argued strongly against the notion of a field cipher that would simply resist solution long enough for the orders it transmitted to be carried out. This was not enough, he said, declaring that "the secret matter in communications sent over a distance very often retains its importance beyond the day on which it was transmitted." He was on the side of the angels, but a practical field cipher that is unbreakable was not possible in his day, nor is it today, and so military cryptography has settled for field ciphers that delay but do not defeat cryptanalysis.

Perhaps the most startling requirement, at first glance,

was the second. Kerckhoffs explained that by "system" he meant "the material part of the system; tableaux, code books, or whatever mechanical apparatus may be necessary," and not "the key proper." Kerckhoffs here makes for the first time the distinction, now basic to cryptology, between the general system and the specific key. Why must the general system "not require secrecy," as, for example, a codebook requires it? Why must it be "a process that. . . our neighbors can even copy and adopt"? Because, Kerckhoffs said, "it is not necessary to conjure up imaginary phantoms and to suspect the incorruptibility of employees or subalterns to understand that, if a system requiring secrecy were in the hands of too large a number of individuals, it could be compromised at each engagement in which one or another of them took part." This has proved to be true, and Kerckhoffs' second requirement has become widely accepted under a form that is sometimes called the fundamental assumption of military cryptography: that the enemy knows the general system. But he must still be unable to solve messages in it without knowing the specific key. In its modern formulation, the Kerckhoffs doctrine states that secrecy must reside solely in the keys.

Had Kerckhoffs merely published his perceptions of the problems facing post-telegraph cryptography and his prescriptions for resolving them, he would have assured a place for himself in the pantheon of cryptology. But he did more. He contributed a technique of cryptanalysis that is of supreme importance today. Called "superimposition," it constitutes the most general solution for polyalphabetic substitution systems. With few exceptions, it lays no restrictions on the type or length of keys, as does the Kasiski method, nor on the alphabets, which may be interrelated or entirely independent. It wants only several messages in the same key. The cryptanalyst must align these one above the other so that letters enciphered with the same keyletter will fall into a single column. In the simplest case, that of a running key (a very long continuous text used as a key, as a novel) that restarts with each message, he can do this simply by placing all the first letters in the first column, all the second letters in the next column, and so on.

Kerckhoffs demonstrated this procedure with 13 short messages enciphered with a long key. He superimposed his first five cryptograms like this:

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | 1 |
| | | | | 0 | | 21 | 4 | 15 |
| | | 4 | | 11 | | 3 | . . | |
| *Mess* | | | | | | | | M |
| *age 1* | J | | | | | | T | |
| | | B | | F | | M | . . | |
| *Mess* | | | | | | | | R |
| *age 2* | J | | *P* | | | | E | |
| | | | | B | | W | . . | |
| *Mess* | | | | | | | | G |
| *age 3* | | | | | T | | J | |
| | | H | | | | V | . . | |
| *Mess* | | | | | | | | G |
| *age 4* | r | | | | | | H | . |
| | | R | | W | | E | . | |
| *Mess* | | | | | | | | V |
| *age 5* | | | | | | | X | . |
| | | H | | J | | Z | . | |

Now, since all these messages were enciphered with the same keytext, all the hidden plaintext letters in the first column were enciphered by the same keyletter, which means that they have been enciphered in the same cipher-text alphabet. Consequently, all the plaintext a's will have the same ciphertext equivalent, all the plaintext *b's* will likewise have their own unvarying ciphertext equivalent, and so on. Likewise, each ciphertext letter represents only one plaintext letter. This holds true for each column. Each column may thus be attacked as an ordinary monalpha-betic substitution, just as Kasiski did with identically enciphered letters in a periodic polyalphabetic.

In cases where the key does not start over again with each message, the cryptanalyst may line up repetitions in several messages to obtain a proper superimposition.

It is ironic that the most lasting work of a man whose ideals were as cosmopolitan as Kerckhoffs' should have had nationalistic results. Yet perhaps the most immediate consequence of *La Cryptographic militaire* was its giving France a commanding lead in cryptology. The flowering of cryptologic literature that it engendered there reflected that nation's profound understanding of the subject. And French solution of Italian and German diplomatic codes, which allowed her to read critical German messages on. the very eve of World War I, demonstrated her practical capabilities. The army at the same time prepared, through a Military

Cryptography Commission, for the solution of enciphered German radio messages. These would be intercepted by the major fortress stations in the northeast that faced Germany.

Of the other major countries of Europe, only Austria-Hungary had prepared cryptanalytically for the war. The Dual Monarchy began to intercept the radio messages of her arch-rival Italy in 1908. In 1911, with the Italo-Turkish conflict, Captain Andreas Figl became the chief of a newly

formed cryptanalytic bureau that was to do remarkable work. Other nations remained ignorant. England, Germany, and Russia made no preparations whatsoever for military radio intelligence. It was about their only failure in readying for the expected conflict. Finally, in an obscure corner of the Balkans, someone helpfully slew an archduke, and the nations leaped recklessly into the bloody cockpit of war.

## 8. Room 40

BEFORE DAWN on the morning of August 5, 1914, the first day of a world war that was to convulse country after country and to end the lives of millions, an equipment-laden ship slid quietly through the black and heaving waters of the North Sea. Off Emden, where the Dutch coast joins the German, she dropped some grappling gear overboard with a dull splash, and shortly there rose dripping from the sea great snakelike monsters, covered with mud and seaweed. Grunts of men, chopping sounds—and soon they were returned, severed and useless, to the depths. These were Germany's transatlantic cables, her chief communications lifelines to the world, and the vessel was the British cable ship *Telconia.* Though the Committee of Imperial Defence never dreamed of it when it planned the move in 1912, the cutting of these cables, England's first offensive action of the war, forged the first link in a chain that helped to end it.

Germany was now forced to communicate with the World beyond the encircling Entente by radio or over cables controlled by her enemies. She thus delivered into the hands of her foes her most secret and confidential plans, provided only that they could remove the jacket of code and cipher in which Germany had encased them. It Was an opportunity for which England was unprepared, but of which she promptly availed herself.

On that first day of the war, the director of naval intelligence, Rear Admiral Henry F. Oliver, walked to lunch With the only man at the Admiralty to take any interest in cryptology, the director of naval education, Sir Alfred

p

Ewing. A few months before, Ewing had devised what he later called a "futile" ciphering mechanism, and he had spoken to Oliver about new methods of constructing ciphers. Oliver mentioned that some naval and commercial radio stations were sending to the Admiralty some messages in code that they had picked up and that these were accumulating on his desk. The Admiralty had no department to deal with enemy cryptograms, he said. Ewing was at once interested, and when he saw the messages that afternoon he recognized that they were probably German naval signals and that their solution could be of great value. He promptly undertook the task.

Ewing was then 59, a short, thickset Scot with blue eyes beneath shaggy eyebrows, a quiet voice, and the manner of a benign physician. He had been knighted three years before for his contributions to science, which included pioneering studies of Japanese earthquakes, of magnetism, and of mechanical lagging effects in stressed materials (now known by a word he coined, "hysteresis"), and for his public services, notably his naval education directorship. He was to become president of the British Association for the Advancement of Science and perhaps his country's greatest living expert on mechanical science. And now he was about to found a cryptanalytic bureau that was to become almost legendary and to exert a direct and noticeable effect upon the course of history.

He began by boning up on ciphers in the stacks of the British Museum library and on the construction of codes at Lloyd's of London and at the General Post Office, where commercial codebooks were on file. He called in four teachers at the naval colleges at Dartmouth and Osborne, A. G. Denniston, W. H. Anstie, E. J. C. Green, and G. L. N. Hope, all friends of his with a good knowledge of German, and, sitting together around the table in his office, they inspected the incomprehensible lines of letters and numbers with only the feeblest general idea on how to begin.

None of the small band of pioneers had had any real previous knowledge of cryptanalysis, and they made only antlike progress in those first weeks. But Ewing was exhilarated by the job, and it was not until October 25 that he took a Sunday off. By then, England had had a stroke of fortune that gave such an impetus to its cryptanalytic work that it remained far ahead of its enemies through the rest

of the war. What happened has best been told in his own style by the minister who then headed the Admiralty, the First Lord, Winston Churchill:

> At the beginning of September, 1914, the German light cruiser *Magdeburg* was wrecked in the Baltic. The body of a drowned German under-officer was picked up by the Russians a few hours later, and clasped in his bosom by arms rigid in death, were the cypher and signal books of the German Navy and the minutely squared maps of the North Sea and Heligoland Bight. On September 6 the Russian Naval ATTACHÉ came to see me. He had received a message from Petrograd telling him what had happened, and that the Russian Admiralty with the aid of the cypher and signal books had been able to decode portions at least of the German naval messages. The Russians felt that as the leading naval Power, the British Admiralty ought to have these books and charts. If we would send a vessel to Alexandrov, the Russian officers in charge of the books would bring them to England. We lost no time in sending a ship, and late on an October afternoon Prince Louis [of Battenberg, First Sea Lord] and I received from the hands of our loyal allies these sea-stained priceless documents.

The date was October 13. But even this astounding windfall—the luckiest in the whole history of cryptology—did not enable Ewing's team to read the German naval messages, for the four-letter codewords in that book did not appear in the dispatches. Finally, Fleet Paymaster Charles J. E. Rotter, a principal German expert, discovered that the code had been superenciphered with a monoalphabetic substitution. Solution of such a superencipherment is not too difficult a problem with the codebook in one's possession. As in ordinary plaintext, certain codewords recur more frequently than others and in familiar clusters, letters in one codeword reappear in others in different arrangements, and the codewords themselves possess some structural regularities: in the case of the German naval code, consonants alternated with vowels in the four-letter codewords. When these characteristics are known, the crypt-analyst can spot them almost as well as the more pro-

nounced ones of ordinary language, and can exploit them to solve the superencipherment.

So green were the British cryptanalysts that it took them almost three weeks before they began reading portions of some German naval messages. These, Churchill says, "were mostly of a routine character. 'One of our torpedo boats will be running out into square 7 at 8 p.m.,' etc. But a careful collection of these scraps provided a body of information from which the enemy's arrangements in the Heligoland Bight [bordering the northwest German coast] could be understood with a fair degree of accuracy."

By this time, Ewing's staff had grown to such an extent that they crowded his office, and they were continually irked by having to put their work out of sight when he had visitors on educational subjects. So about the middle of November the entire cryptanalytic group moved to Room 40 in the Old Buildings of the Admiralty. This was a large room with a small room adjoining, with a camp bed for tired staffers. Room 40, O.B., had the advantage of being out of the main stream of Admiralty traffic, yet being relatively handy to the Operations Division, which received its output. Though the cryptanalysts were later designated as I.D. 25 (section 25 of the Intelligence Division), "Room 40" was so convenient and so innocuous a name that it soon became the common identification for the organization. The name stuck even when I.D. 25 moved into larger quarters.

Meanwhile, naval intelligence was building up activities concomitant to cryptanalysis. Major radio direction-finding stations were—largely thanks to Oliver's foresight—set up at Lowestoft, York, Murcar, and Lerwick; they fed their readings into Whitehall, where they proved of immense help in locating the German fleets and the movement of the U-boats. There was no way of avoiding a fix except by maintaining radio silence. This fact was of course known to the Germans, and in view of it England made no attempt to keep its direction-finding activity secret, using it as a smokescreen for its less obvious and more valuable cryptanalytic work. Two other sources of radio intelligence were the identification of ships' radio call-signs and the recognition of a radio operator's "fist," or characteristic way of sending Morse code.

After Jutland, the German emphasis on submarine warfare intensified Room 40's concentration on the U-boat

messages. These were encoded in the four-letter code of the High Seas Fleet, but were superenciphered by columnar transposition. The Germans called the one for the regular U-boats "gamma epsilon" and that for the larger cruising submarines, whose keyword differed, "gamma u." Keywords changed often but not daily. Three or four staffers specialized in this; they became so adept that they usually managed not only to restore the scrambled codewords to their original form but even to recover the keyword for the transposition tableau. The solutions greatly assisted British operations, and eventually the Germans could no longer chalk off as coincidental the repeated apparitions of substantial British units athwart their course. In August of 1916, they changed their code. But Room 40's direction-finding and call-sign sections were so well oiled that they nevertheless maintained a fair flow of intelligence. More help came from divers who recovered codes from sunken U-boats.

These finds helped the cryptanalysts in reading the increasing volume of enemy messages. Room 40 was now approaching the height of its power. Intercepts poured in through the pneumatic tube so fast that at times the discharge of its small containers sounded like a machine gun. (After the war it was estimated that from October, 1914, to February, 1919, Room 40 had intercepted and solved 15,000 German secret communications.) Work went on round the clock on the naval messages, even during the Zeppelin bombings, when the lights were dimmed behind the close-fitting dark blinds. The staff was further increased by wounded officers and by German university scholars, many of whom were commissioned in the Royal Navy Volunteer Reserve so that they could wear uniforms to forestall icy looks from the public. Women were enlisted to free cryptanalysts from clerical tasks.

The most important personnel change came with the retirement of Ewing and his replacement as immediate overseer of Room 40 by the director of naval intelligence. Captain William Reginald Hall, R.N., unforgettably impressed all who met him. A dapper, alert man with a perfectly domed, prematurely bald head and a large hooked nose, Hall, then in his middle forties, looked like a demonic Mr. Punch in uniform. The American ambassador, Walter Hines Page, summed him up best in a letter to President Woodrow Wilson: "Hall is one genius that the

war has developed. Neither in fiction nor in fact can you find any such man to match him. Of the wonderful things that I know he has done, there are several that it would take an exciting volume to tell. The man is a genius—a clear case of genius. All other secret-service men are amateurs by comparison."

At about half-past ten on the morning of January 17, 1917, the Reverend William Montgomery, a thin, gray-haired scholar of the early church fathers who was serving as a cryptanalyst in the diplomatic section of Room 40, came to tell Hall of what looked like an important message. Montgomery's instincts were right. The cryptogram that he and a youthful colleague, Nigel de Grey, had partially read was to become the single most far-reaching and most important solution in history.

The message was a long one, consisting of about a thousand numerical codegroups. Dated at Berlin January 16, it was addressed to the German ambassador in the United States, Count Johann Heinrich Andreas von Bern-storff, and the two cryptanalysts recognized that it was encoded in a German diplomatic code known as 0075, upon which they had been working for six months. Room 40 knew from its analyses that 0075 was one of a series of two-part codes that the German Foreign Office designated by two zeros and two digits, the two digits always showing an arithmetical difference of 2. Among the others, some of which Room 40 had solved, were 0097, 0086, which was used for German missions in South America, 0064, used between Berlin and Madrid and perhaps elsewhere, 0053, and 0042. Code 0075 was a new code that the German Foreign Office had first distributed in July of 1916 to German missions in Vienna, Sofia, Constantinople, Bucharest, Copenhagen, Stockholm, Bern, Lugano, The Hague, and Oslo. Somehow the British obtained copies of enough of the telegrams in this code to enable Montgomery and de Grey, whose assignment it probably was, to make a start in breaking it. In November, Room 40 began intercepting messages to the German embassy in the United States in the same code, and if Hall guessed that the code and the keys to the superencipherment that it sometimes used had been sent across the Atlantic on the second voyage of the cargo U-boat *Deutschland,* which

docked at New London on November 1, 1916, he would have been right.

Montgomery and de Grey could read only parts of the long message. But they could see that it was a double-decker, consisting of Berlin's messages Nos. 157 and 158 to Bernstorff. They could read the signature of the German Foreign Minister, Arthur Zimmermann. As far as they could extricate its sense on the basis of their partial solution of 0075, the second message read:

> Most secret for your Excellency's personal informa-, tion and to be handed on to the Imperial Minister in (? Mexico) with Telegram No. 1 (...) by [a] safe route.
>
> We propose to begin on the 1st February unrestricted submarine warfare. In doing so, however, we shall endeavor to keep America neutral. (?) If we should not (succeed in doing so) we propose to (? Mexico) an alliance upon the following basis:
>
> [joint] conduct of the war.
>
> [joint] conclusion of peace.
>
> (...)
>
> Your Excellency should for the present inform the President [of Mexico] secretly (? that we expect) war with the U.S.A. (possibly) (. . .) (Japan) and at the same time to negotiate between us and Japan. (Please tell the President) that (. . .) or submarines (. . .) will compel England to peace in a few months. Acknowledge receipt.
>
> Zimmermann.

Montgomery handed this fragmentary solution to Hall, who stared down at the phrases that seemed to jump off the page at him: "unrestricted submarine warfare," "war with the U.S.A.," "propose ... an alliance." He realized at once that here was a weapon of enormous potentiality. He urged Montgomery to hurry the solution, ordered all copies except the original message and a single solution burned, and, without a word to the Foreign Office, sat down by himself to contemplate the situation.

It was as bleak as that winter's day. The war that everyone had expected would last only a few weeks had now dragged into its third year. Nor was there any prospect of an end. France had expended half a million lives at Verdun

and only succeeded in restoring the battle line to where it was ten months before. England, which had lost 60,000 men at the Somme in a single day, struggled to gain a few yards of shell-blasted earth, then fell back exhausted. The Hindenburg line remained unbreached. Rumania, a new ally, had been quickly overrun, and Russia, the colossus of the east, was virtually defeated. The stepped-up U-boat campaign increased the economic pressure on the Allies. Worst of all, despite the provocation of the *Lusitania* sinking and despite the tug of ancient common ties, the United States, guided by a President who had just won reelection on the slogan "He kept us out of war," remained obstinately neutral.

Things were no better in Germany. Her initial offensive had stalled at the Marne and her gray-coated troops had been locked in the futile trench slaughter ever since. Civilians were living on potatoes—a result of the stranglehold of the British blockade. Fifteen-year-olds were being conscripted. Greece and Portugal had recently entered the war against her. Like the Allies, she could see no immediate hope for victory.

Except one.

Unleash the submarines, the generals cried, and England would soon be "gasping in the reeds like a fish." The blockaders would become the blockaded. For months the generals had hammered away on this theme, and, as the signs of exhaustion multiplied, they finally prevailed. Foreign Minister Zimmermann, who had long opposed the idea, fell in line. But this big jolly bachelor, the first to break the Junker barrier in the higher regions of the Kaiser's officialdom, perceived that the repeated sinkings of American vessels would sooner or later torpedo American neutrality, and he bethought himself of a scheme to counter this danger. He proposed a military alliance with Mexico, then particularly hostile to the imperialistic Norte-americanos as a result of Pershing's punitive expedition into Mexican territory. He sweetened the proposition with an offer of money and the possibility of support from Japan, standing at America's back, and with still more anti-Yankee inducements.

Unable to deal through the Mexican ambassador, who was in Switzerland, Zimmermann sent his proposal to his minister in Mexico, Heinrich J. F. von Eckardt, by way of Washington. To ensure that it would get there, he routed

jt two ways, both monitored by Britain. The cruise of *Telconia* was paying off.

One way was called the "Swedish Roundabout" by the British. Sweden, which was neutral in favor of Germany, had since early in the war helped the German Foreign Office get messages past the British cable blockade by sending them as her own. British censorship detected this practice. When Sweden complained in the summer of 1915 that Britain was delaying her messages, Britain informed her that it had positive knowledge of the unneutral practice. • The Swedish government admitted this and promised that it would no longer send any German messages to Washington. It did not. Instead, it sent them to Buenos Aires. Here they were transferred from Swedish to German hands and then forwarded to Washington. This was a circuitous route of about 7,000 miles, half of them in flat violation of the prerogatives of a nonbelligerent.

But the cable from Stockholm to South America touched at England. Germany feared that British censorship might recognize the German codegroups in the Swedish messages and would stop the dispatches. So the German Foreign Office disguised the codegroups by enciphering them. This was done with Code 13040 in messages to Latin America and to Washington. Unfortunately for the Germans, the superencipherment did not obliterate all traces of the underlying code, which employed a distinctive mixture of 3-, 4-, and 5-digit codegroups. These traces aroused the suspicious of the ever-alert Room 40; it resolved the superencipherment, and Code 13040 reappeared. Room 40 then looked closely at other official Swedish messages. Many of them proved to be German as well; concealed under one superencipherment, for example, they found Code 0075. But this time England entered no protest. Hall perceived that it was more advantageous to listen to what the Germans were saying than to stop them from talking.

The second route that Zimmermann used was of such simplicity, perfidy, and barefaced gall that it probably remains unequaled in the annals of diplomacy. It had its inception in the pompous mind of Colonel Edward M. House, President Wilson's alter ego and a major exponent of personal diplomacy. On one of his missions to Europe in 1915, House arranged to have coded reports from the embassies cabled directly to him, bypassing the State Department. When, on December 27, 1916, Ambassador

Bernstorff discussed a new peace attempt by Wilson with House, he pointed out that the chances would be improved if his government could communicate directly with Wilson through House. House checked with the President. The next day Wilson permitted the German government to send messages in its own code between Washington and Berlin under American diplomatic auspices—an arrangement that was, at best, simpleminded, and that, furthermore, contravened the accepted international practice of requiring the messages to be submitted in clear for transmission in American code.

Germany availed herself of this arrangement to make America seal her own doom by letters she herself bore. Under the aegis of American sovereignty, Zimmermann sent his message striking at that sovereignty. It was delivered to the American embassy in Berlin at 3 p.m. January 16. It could not go direct to Washington, but had to be sent first to Copenhagen—and then to London. Only from there could it go to Washington. Consequently Britain seized this copy as well. Room 40 was "highly entertained" at the sight of the German code in an American cable, but again did not protest.

With two copies of the same text helping to eliminate garbles, Montgomery and de Grey rammed into the cryptogram. De Grey, though at 30 the younger of the two, had been in Room 40 the longer. Slightly built, rather handsome, with dark hair and brown eyes and chiseled, movie-star features, an Eton graduate, he was descended from the peerage as the grandson of the fifth Baron Walsingham (no relation to Sir Francis Walsingham). He had worked for the prestigious publishing house of William Heinemartn for seven years before the war, when he joined the Royal Naval Air Service. He came to Room 40 in 1915.

Montgomery was 45 at the time of his work on the Zimmermann telegram. A Liverpool shipowner's son who studied in private schools or under tutors in England, France, and Germany, he took a bachelor of divinity degree at Presbyterian College, London. But his health prevented an active pastorate and he became a member of St. John's College at Cambridge University. He specialized in early church history, editing the *Confessions* of St. Augustine for the Cambridge Patristic Series and writing a study on the life and thought of the African father. His most memorable work, however, was as a translator. It was said of his

translation of Albert Schweitzer's *The Quest of the Historical Jesus* in 1910 that "no German work has ever been rendered into English so idiomatically and yet so faithfully." A modest, reticent man, Montgomery entered the censor's office in 1916, and later that year moved to Room 40.

While in Room 40 his familiarity with Scripture unriddled a problem that had baffled most of the other staffers. A Sir Henry Jones had received a blank postcard from Turkey addressed to him at 184 King's Road, Tighna-bruaich, Scotland. Sir Henry knew that the card was from his son, who had been captured by the Turks, but Tighna-bruaich is a small village, with no King's Road and so few houses that no number would have been needed in any case. The card found its way to Room 40, where nobody seemed able to ascertain what Sir Henry's son was trying to tell him. Finally Montgomery suggested a reference to chapter 18, verse 4, of one of the books of Kings. Second Kings shed no light, but First Kings revealed that "Obadiah took a hundred prophets, and hid them fifty in a cave, and fed them with bread and water." Montgomery interpreted this to mean that Sir Henry's son was safe with other prisoners but in need of food—and this proved to be the case.

But the solution of the Zimmermann telegram required more than a flash of inspiration. It demanded the reconstruction of Code 0075, a two-part code of 10,000 words and phrases numbered from 0000 to 9999 in mixed order. Since a code is, in a sense, a gigantic monoalphabetic substitution, the establishment of plaintext equivalents is the "only" task involved. But where the cryptanalyst of cipher deals with only 26 such elements, the cryptanalyst of code must keep his eye on hundreds or thousands, whose characteristics, moreover, because of their reduced frequency, are much scantier and more diffuse than the sharply defined traits of letters.

Solution usually begins with the identification of the groups meaning *stop.* Groups that recur near the end of telegrams are likely candidates. The identification of *stop* or *period* is often aided because often only a few of the many code equivalents are employed. Code clerks, referring frequently to *stop,* come to memorize one or two of its codegroups; they then simply use these groups in encoding instead of hunting up a different one in the codebook.

Indeed, cryptanalysts familiar with a given embassy's messages can often tell when a new code clerk has been hired by the sudden efflorescence of new equivalents for *stop!*

The identification of the stops outlines the structure of the message. In English messages, nouns, as the subjects of sentences, will often appear directly after stops. In German, where the predicate often comes at the end of the sentence, the codegroup immediately preceding a stop may be a verb. Other clues come from the stereotyped expressions that diplomats so love in their dispatches: "I have the honor to report to Your Excellency. ..." Collateral information is of very great value.

The first tentative identifications are usually written in pencil for easy erasing, and such are called "pencil groups." Eventually, further traffic confirms them and they become "ink groups." Solution proceeds much more rapidly if a code is one-part. If codegroup 1234 represents a word beginning with *d,* then 5678 must represent one farther back in the alphabet; this both rules out some guesses and suggests others. Sometimes the meaning of a codegroup can be indicated rather precisely by its location between two ink groups. This is not possible with a two-part code, where the code and plain equivalents are matched in an absolutely arbitrary fashion. Code 0075 was of this type. It required more traffic for its solution than a one-part code, and the identifications came more slowly and with greater difficulty. It had been in service on the Continent for only half a year—not a very long time for a diplomatic code—and portions of many messages remained unreadable.

As more traffic came in (including now the messages to and from Bernstorff), Montgomery and de Grey, working night and day, filled in more and more groups, ever more rapidly. On January 28, de Grey brought Hall part of Bernstorffs protest against Zimmermann's plan of unrestricted submarine warfare, which, to the ambassador's dismay, had been announced to him in message No. 157, the first part of the double-decker. Bernstorff argued vigorously against this plan, for he felt that it negated all his efforts to bring about a detente between the two countries and that it would drive the United States into the war on the side of the Allies.

And in fact, on February 3 Wilson announced to Congress that he was breaking diplomatic relations with Germany, as he had said he would the previous April if

Germany continued its course of submarine warfare. Though he added that "only actual overt acts" on Germany's part would make him believe that she really would sink neutral vessels on the high seas, it must have seemed to the war-weary Allies that now, at last, within a few days or a fortnight at most, the United States would enter the war. Day by day, they awaited the final inevitable step.

While waiting, Room 40 continued its work on Code 0075. De Grey had taken to Hall Bernstorff's message giving details of his interview with Wilson severing relations. Recovered codegroups were substituted into the Zimmermann telegram, and on February 5 Hall was able to show a more fully solved version of it to Lord Hardinge at the Foreign Office.

Hall had realized from the first day that Montgomery had brought him the first sketchy solution of the Zimmermann telegram that he had in it a propaganda weapon of titanic proportions. Exposure of this German plot directed against the United States would, in the present circumstances, almost certainly compel that nation to declare war on Germany. This was an immensely strong argument for showing it to the Americans. But for the moment, at least, even stronger considerations militated against it. First, Room 40 and its cryptanalytic capabilities was one of Britain's darkest secrets. How could she disclose the message without Germany's guessing that her codes were being read? Britain might minimize the risk by hinting that the plaintext had been stolen, but the danger would still remain that Germany would suspect the truth, change her codes, and deprive Britain of her most valuable intelligence. In the second place, to reveal the message, Britain would have to admit that it had been supervising the code telegrams of a neutral: Sweden. It would not require much wit for the Americans to surmise that England might also be supervising the code telegrams of another neutral: the United States, which, like Sweden, was working as a messenger boy for the Germans and had, in fact, transmitted this very message. This realization would both embarrass and anger the United States and would not conduce to pro-Allied feelings. In the third place, the solution was still not complete. The missing portions would inevitably raise doubts about the validity of the solution and so weaken its impact. Perhaps the British had failed to solve a word like "not" that would completely alter the sense,

the arguments would run. Perhaps the British had not even correctly solved the portion that they were offering as evidence of German duplicity. Moreover, the gaps would shout "codebreaking," preventing any subterfuges about captured codes or a stolen message and exposing the very secret Britain sought to conceal.

But the most powerful argument against disclosure of the German plot, with all the attendant difficulties, was that events might make it unnecessary. Relations had been severed between Germany and the United States. American public opinion seemed to be turning increasingly against Germany. Shipping dared not sail; ports were congested; men were laid off; business languished. Bitterness was growing. It seemed only a matter of a short while until the declaration of war. And so the British continued to wait, and to hope.

Hall, however, while waiting for events to dictate, did not remain idle. His job was only half done if he merely solved the Zimmermann telegram without making it ready for use by his government. Consequently, he conceived a plan that at one stroke might resolve the three difficulties connected with the telegram's exposure, in what still appeared the unlikely event that that might be necessary. He reasoned that the telegram as received in Mexico would differ in small but significant details from the telegram as sent from Berlin. The date would almost certainly be different, and probably the serial number as well. The preamble addressed to BernstorfF ordering him to forward the message would of course be omitted. If Hall could produce the copy from Mexico, perhaps the Germans would spot these slight variations and infer that the plaintext had been betrayed on the American continent and would not change their codes. Other collateral details might confirm a tale of a Mexican theft to the Americans. Moreover, Room 40 perhaps knew, from its numerous solutions of German messages via the Swedish roundabout, that the German mission in Mexico had not used Code 0075 and probably did not hold it. Bernstorff might then have had to re-encode the Zimmermann telegram in another code, which Room 40 might have solved more completely than 0075 and which might therefore enable it to fill in the missing portions in its solution.

On February 5, therefore, Hall began trying to get a copy of the Zimmermann telegram as received in Mexico.

An English agent known only as T obtained from the Mexico City telegraph office a copy of the message that Bernstorff had sent to Eckardt by Western Union. Soon Hall had it.

It proved him right in every one of his assumptions. Eckardt did not have Code 0075, and so Bernstorff had had to recede the dispatch in one that Eckardt did have. This was Code 13040, which was an older and simpler code than 0075 and whose superencipherment had led to the discovery of the Swedish roundabout. It had been distributed to German missions in Central and South America between 1907 and 1909 and to Washington, New York, Havana, Port-au-Prince, and La Paz in 1912. Its basic repertory contained about 25,000 plaintext elements with a fair number of homophones—Bernstorff's telegram alone employed six different groups for *zu*—and proper names took up a huge section of 75,000 codenumbers. But Code 13040 was a cross between one-pa'rt and two-part codes. In the encoding section, blocks of several hundred code-numbers in numerical order stood opposite the alphabetized plaintext elements, but the blocks themselves were in mixed order. A skeleton code, made up from a few groups from Bernstorff's encoding, will illustrate this:

| *encoding* | *decoding* |
|---|---|
| 13605 Februar | 5144 wenigen |
| 13732 fest | 5161 werden |
| 13850 fmanzielle | 5275 Anregung |
| 13918 folgender | 5376 Anwendung |
| 17142 Frieden | 5454 ar |
| 17149 Friedenschluss | 5569 auf |
| 17166 fuhrung | 5905 Krieg 17214 Ganz geheim 17388 Gebeit |
| 4377 geheim | |
| 4458 Gemeinsame | |

The solution of such a hybrid code stands midway in difficulty between the two pure types: harder than a one-part code but easier than a two-part. The large orderly segments considerably help the cryptanalyst, though his guesses are not as delimited as in a one-part code. For example, the cryptanalyst could not assume, as he could in a one-part solution, that a codegroup for *Krieg* will be

higher in number than the codegroup for *Februar.* But if he knows that *Februar* is 13605 and *finanzielle* is 13850, he will know that the codegroup for *fest* must almost certainly fall somewhere between the two. His identifications thus come with greater speed and certainty.

[Codebreakers 114.jpg]

*The Zimmermann telegram as re-encoded in Washington into Code 13040 and forwarded to Mexico*

Owing to this weakness, and to the fact that they had had all of the war to work on a great volume of messages, the codebreakers of Room 40 had recovered most of Code 13040's commonly used groups. They could consequently read all or nearly all of Bernstorff's message to Eckardt, and in those few places where a rare proper name or syllable might have been used for the first time, the partial alphabetical arrangement afforded a strong check on their guesses. This eliminated the problem of having only a partial solution. In addition, it confirmed their almost-

complete solution of the original Berlin-to-Washington message and added a few new values to their reconstruction of Code 0075.

The cryptanalysts also found the slight changes in heading that Hall had foreseen. Bernstorff had deleted the Foreign Office preamble and substituted one of his own: "Foreign Office telegraphs January 16: No. 1. Most Secret. Decode yourself." He replaced the Berlin-Washington serial number with a Washington-Mexico City serial number, which was 3. And finally, his message was dated January 19, which, due to the numerous steps in the complicated transmission routes, differed from the January 16 date that the original German text bore.

Fairly early in February, it seems, Hall' was ready. With a stroke bordering on genius, he had done his job. His must stand as one of the most subtly dissembling moves in the whole history of espionage. It was now possible to give the message to the Americans, should that prove necessary, with as little risk as possible to Britain's intelligence sources. But though Hall had covered his tracks fairly well, it remained possible that the Germans might guess the truth. Events might yet make it unnecessary to chance this. So Britain held the message and waited.

And waited. The days passed. On the Western Front the lifeblood of the Empire and of the French republic trickled into the earth. The armies shuddered in mortal combat. Still there came no sign that America was going to enter the war. Though it seemed that Germany's announcement of unrestricted torpedoings of American ships had made, as Bernstorff himself had warned in cables read by Room 40, "war unavoidable," the American President seemed unable to do what the British thought that honor, self-respect, and the whole course of recent actions made obligatory. Even Ambassador Page, a long-time friend of the President and a wholehearted sympathizer with the Allied cause, was irked enough to note in his diary, "The danger is that with all the authority he wants (short of a formal declaration of war) the President will again wait, wait, wait—till an American liner be torpedoed! Or till an attack is made on our coast by a German submarine!" Evidently Wilson was waiting for the "overt acts" that he had mentioned in his address to Congress. But perhaps Germany would not actually be so rash as to torpedo American ships and thereby—Britain thought—cut her own

I

throat. More days passed. The Germans did nothing. Tension mounted. The situation was, a British diplomat in America reported, "much that of a soda-water bottle with the wires cut but the cork unexploded."

It exploded on February 22, 1917. Unable to wait any longer, the British gave the cork a push. Hall, with Foreign Office approval if not under its orders, showed the Zimmermann telegram to Edward Bell, a secretary of the American embassy who maintained liaison with the various intelligence offices of the British government. He read an astounding tale of German intrigue against his country:

> We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis:
>
> Make war together, make peace together, generous financial support, and an understanding on our part that Mexico is to reconquer the lost territory in Texas, New Mexico and Arizona. The settlement in detail is left to you.
>
> You will inform the President [of Mexico] of the above most secretly, as soon as the outbreak of war with the United States of America is certain and add the suggestion that he should, on his own initiative, invite Japan to immediate adherence and at the same time mediate between Japan and ourselves.
>
> Please call the President's attention to the fact that the ruthless employment of our submarines now offers the prospect of compelling England in a few months to make peace.
>
> Zimmermann.

Bell did not believe it. The notion that anyone in his right mind would consider giving away a chunk of the continental United States was simply too preposterous. But Hall convinced him of its authenticity, and the two went over to Grosvenor Square. When Page saw the message, he realized at once that the entry into war on England's side, which he had so single-mindedly pursued and the

President had so obstinately opposed, was at last delivered into his hands. Hall, Bell, Page, and Irwin Laughlin, first secretary of the embassy, spent the day trying to decide how best to instill confidence in the telegram's genuineness, to minimize incredulity, and to maximize its impact. They decided that the British government should officially present the telegram to Page, and in his room at the Foreign Office the next day Arthur Balfour, now secretary of state for foreign affairs, formally communicated it to Page in a moment that Balfour later confessed was "as dramatic a moment as I remember in all my life."

Page worked all night to draft a covering message explaining how the telegram was obtained. At 2 a.m. February 24 he cabled, "In about three hours I shall send a telegram of great importance to the President and Secretary of State," but it was not until 1 p.m. that the Zimmermann telegram, with his explanation, was transmitted. He gave the President the collection of half-truths that Hall had given him—for Hall naturally withheld the deep secret of British cryptanalytic ability, particularly since it might start the Americans wondering whether Britain was reading their code messages as well:

> Early in the war the British government obtained possession of a copy of the German cipher code used in the above message and have made it their business to obtain copies of Bernstorffs cipher telegrams to Mexico, among others, which are sent back to London and deciphered here. This accounts for their being able to decipher this telegram from the German government to their representative in Mexico, and also for the delay from January 19th until now in their receiving the information. This system has hitherto been a jealously guarded secret and is only divulged to you now by the British government in view of the extraordinary circumstances and their friendly feeling toward the United States. They earnestly request that you keep the source of your information and the British government's method of obtaining it profoundly secret, but they put no prohibition on the publication of Zimmermann's telegram itself.

Page's pilot telegram rattled the Morse sounders at the State Department at 9 a.m. Saturday, February 24, but

the "telegram of great importance" did not arrive until 8:30 that evening. Frank L. Polk, counselor of the department and acting secretary in the absence of Secretary of State Robert L. Lansing, telephoned to ask the President to expect him and carried the four typewritten yellow sheets across the street to the White House. Wilson, Polk reported, showed "much indignation" on reading it, and wanted to make it public at once. But he agreed to Folk's suggestion to await Lansing's return from a long weekend.

On Tuesday, February 27, Lansing came back from White Sulphur Springs. Polk told him about the Zimmer-mann telegram and showed him an exceptionally long cable of 1,000 codegroups that he had found in the State Department files. It had come for Bernstorff in an American cablegram of January 17 from Berlin and was, Polk felt, almost certainly the coded original. (It was, in fact, the double-decker, which included the Zimmermann telegram.) At 11 that morning, Lansing, armed with this, discussed the whole situation with the President, who, exclaimed "Good Lord!" several times at the outrageous German abuse of the cable privileges he had extended them. He consented to Lansing's plan to release the telegram through the press, which Lansing felt "would avoid any charge of using the document improperly and would attract more attention than issuing it openly." Accordingly, at 6 p.m. the next day, E. M. Hood of the Associated Press was called to Lansing's home, given the message and some background details, and pledged to secrecy on the greatest scoop of the war.

The story broke in eight-column streamers in the morning papers of March 1. "Profound sensation," Lansing noted. The nation gasped. In Congress, the House orated patriotically and passed by 403 to 13 a bill to arm merchant ships. But the Senate, more deliberate, wondered whether the whole thing was not just a crude Allied plot. This reaction had been foreseen. Lansing had asked Page to "Please endeavor to obtain copy of German code from Mr. Balfour," but the British had told him that the code was "never used straight, but with a great number of variations which are known to only one or two experts here. They can not be spared to go to America." This was, of course, another half-truth—the 0075 message was probably superenciphered (the "variations") but the 13040 one was not Polk, meanwhile, exerted tremendous pressure on

Newcomb Carlton, the president of Western Union, and finally managed to get a copy of BernstorfFs telegram to Eckardt despite a federal law protecting the privacy of. telegrams. Lansing appended this codetext to the wire he sent Page at 8 p.m. the day of the expose:

> Some members of Congress are attempting to discredit Zimmermann message charging that message was furnished to this government by one of the belligerents. This government has not the slightest doubt as to its authenticity but it would be of the greatest service if the British government would permit you or someone in the Embassy to personally decode the original message which we secured from the telegraph office in Washington, and then cable to Department German text. Assure Mr. Balfour that the Department hesitated to make this request but feels that this course will materially strengthen its position and make it possible for the Department to state that it had secured the Zimmermann note from our own people.

The message, No. 4494, was received the next day, and by 4 p.m. Page cabled back: "Bell took the cipher text of the German messages contained in your 4494 of yesterday to the Admiralty and there, himself, deciphered it from the German code which is in the Admiralty's possession." In fact Bell wrote only a dozen or so plaintext groups before letting de Grey do the rest in his neat handwriting. Page then sent the German text as decoded by Bell and de Grey. But Lansing and the President had already sent up to the Senate a statement that the government possessed evidence establishing the telegram as genuine, and that no further information could be disclosed.

Everyone already had his own pet theory of how the United States had gotten it. Most popular was the spy story. Most farfetched was that four American soldiers had found it on a German agent trying to cross into Mexico. Most plausible was that the telegram had been found among Bernstorff s effects when his baggage was searched at Halifax after his dismissal. Most amusing were the attacks by the British press on the inefficiency of their secret service and its inferiority to the American. (At least one of these was instigated by Hall himself to throw the theorizers off the scent.)

[Codebreakers 150.jpg]

*Nigel de Grey transcribes the Code 13040 version of the Zimmermann telegram into plaintext for the skeptical Americans*

Wilhelmstrasse, too, wondered where the leak had occurred. Though the message as published in the papers did not carry either BernstorfFs heading or his serial number, it did bear the significant date January 19. "Please cable in same cipher," the Foreign Office purred at a quivering Eckardt, who had already tried to blame Bernstorff for the betrayal, "who deciphered cable dispatches 1 [the Zimmermann telegram] and 11 [ordering Eckardt to negotiate at once for the proposed alliance], how the originals and decodes were kept, and, in particular, whether both dispatches were kept in the same place." Six days later, it picked up the clue that Hall had carefully planted: "Various indications suggest that the treachery was committed in Mexico. The greatest caution is indicated. Burn all compromising material."

Eckardt mustered impressive details to exculpate himself: "Both dispatches were deciphered, in accordance with my special instructions, by [Dr. Arthur von] Magnus [the legation's corpulent secretary]. Both, as is the case with everything of a politically secret nature, were kept from the knowledge of the chancery officials. . . . The originals in both cases were burned by Magnus and the ashes scattered. Both dispatches were kept in an absolutely secure steel safe, procured especially for the purpose and installed in the chancery building, in Magnus' bedroom, up to the time when they were burned." Three days later, he sent in his reserves: "Greater caution than is always exercised here would be impossible. The text of telegrams which have arrived is read to me at night in my dwelling house by Magnus, in a low voice. My servant, who does not understand German, sleeps in an annex. . . . Here there can be no question of carbon copies or waste paper." The shrieks of hilarity that this occasioned Hall, Page, and Room 40 were not heard in Berlin. Its last doubts swept away by the low voice, the steel safe, the scattered ashes, and the non-German-speaking servant, the Foreign Office capitulated. "After your telegram it is hardly conceivable that betrayal took place in Mexico. In face of it the indications which point in that direction lose their force. No blame rests on either you or Magnus."

[Codebreakers 152.jpg]

*"Exploding in his Hands." Cartoon by Rollin Kirby in* The *[New York]* World *just after the Zimmermann telegram was made public*

Meanwhile, the problem of authenticity, which had so troubled the Anglo-American officials and stirred uneasy questions in the Senate and the press, had been eliminated by Zimmermann himself. Completely unexpectedly, he confessed: "I cannot deny it. It is true." Knowledge of the plot had been blandly disavowed by the Mexicans, the Japanese, and Eckardt, and to this day no one knows why Zimmermann admitted it.

His acknowledgment buried the last doubts that the story might have been a hoax.

Suddenly, Americans in the middle of the continent who could not get excited about the distant poppings of a European war jerked awake in the realization that the war was at their border. Texans blinked in astonishment: the

Germans meant to give away their state! The Midwest, unmoved because untouched by the submarine issue, imagined a German-officered army crossing the Rio Grande and swung over to the side of the Allies. The Far West blew up like a land mine at the mention of Japan. Within a month, public opinion crystallized. Wilson, who three months before had said that it would be a "crime against civilization" to lead the nation into war, decided that "the right is more precious than peace" and went up to Capitol Hill on April 2 to ask Congress to help make the world safe for democracy. He cited the Zimmermann telegram in his address:

"That it [the German government] means to stir up enemies against us at our very doors, the intercepted note to the German minister at Mexico City is eloquent evidence. We are accepting this challenge of hostile purpose. ... I advise that the Congress declare the recent course of the Imperial German Government to be in fact nothing less than war against the government and people of the United States, that it formally accept the status of belligerent which has thus been thrust upon it."

The Congress did. Soon the Yanks were coming. The fresh strength of the young nation poured into the trenches of the Western Front to rescue the exhausted Allies. And so it came about that Room 40's solution of an enemy message helped propel the United States into the First World War, enabling the Allies to win, and into world leadership, with all that that has entailed. No other single cryptanalysis has had such enormous consequences. Never before or since has so much turned upon the solution of a secret message. For those few moments in time, the code-breakers held history in the palm of their hand.

## 9. A War of Intercepts

RADIO, envisioned by its inventor as a great humanitarian contribution, was seized upon by the generals soon after its birth in 1895 and impressed as an instrument of war. For it immeasurably magnified the chief military advantage of telegraphy: instantaneous and continuous control of an

entire army by a single commander. By eliminating the need for physical linkage by wire, radio speeded communication between headquarters, joined through the ether units that could not connect by wire because of distance, terrain, hostile forces, or rapid movement, opened communications with naval and air forces, and eased the economic burden of producing immense quantities of wire. But few blessings are unmixed. Just as the telegraph had made military communications much more effective but had also increased the possibility of interception over that of hand-carried dispatches, so radio's vast amplification of military communications was accompanied by an enormously greater probability of interception. The public, omnidirectional nature of radio transmissions, which makes wireless communication so easy to establish, makes it equally easy to intercept. It was no longer necessary to gain physical access to a telegraph line behind the enemy's front to eavesdrop upon his communications. A commander had only to sit in his headquarters and tune his radio to the enemy's wavelength. Radio thereupon introduced two revolutionary factors in the interception of communications: volume and continuity.

Communications are intercepted, of course, so that they may be submitted to cryptanalysis. Now cryptanalysis has a potential that cryptography does not. Cryptanalysis can alter the status quo. Cryptography can at best conserve it. Cryptanalysis can bring countries into war, engender naval battles and win them, compel besieged cities to yield, condemn queens to death and exile priestly conspirators from their homeland. Cryptanalysis hammers upon the real world. Cryptography does not.

Consequently, the telegraph, which affected only cryptography, had had a wholly internal influence upon cryptology. That a hierarchy of special systems had arisen to displace the nomenclator interested only cryptologists; it did not matter to generals or statesmen. And although the telegraph greatly increased the volume of communications, wiretapping could produce intercepts only at rare and irregular intervals. Cryptanalysis could exercise only transient and haphazard effects. Its potential remained largely unfulfilled. Kerckhoffs accurately regarded it as an auxiliary to cryptography, a means to the end of perfecting military codes and ciphers. Cryptanalysis during the telegraph years was interesting but inconsequential, intriguing but academic—an

I' ideal topic to pass a Victorian tea-time, perhaps, but not

I much more.

; - The radio, however, turned over to the commander a

i copy of every enemy cryptogram it conveyed. It furnished a constant stream of intercepts. And with these, cryptanaly-sis could bear continually upon operations, could be depended upon for information, could affect events decisively. The generals and the statesmen took notice. This was no longer a polite trifling discussion; this had become a weapon, a pursuit entailing all the savagery of warfare and life against death. Radio made cryptanalysis an end in itself, elevating it to an importance coordinate with that of cryptography, if not superior' to it. Radio's impact upon cryptology reverberated in the outside world.

Wire and wireless thus complemented one another. The telegraph created modern cryptography; the radio, modern cryptanalysis. The one developed cryptology internally, the other externally. The telegraphy had given cryptology shape and content; now the radio carried it out into the arena of life. One gave it form; the other, meaning. The radio completed the work that the telegraph had begun. And so it was that radio, first widely used in the Great War of 1914 to 1918, brought cryptology to maturity.

To the right of the imposing stone A.E.F. headquarters building at Chaumont stood an undistinguished, single-story barracks of glass and concrete. Sometimes called the "Glass House," the caserne housed the other half of the American cryptologic effort, the Radio Intelligence Section, G.2 A.6.

Its chief, Major Frank Moorman, 40, a native of Michigan, was a blue-eyed, brown-haired Regular Army man who had worked his way up through the infantry ranks from private. He was a 1915 graduate of the Army Signal School and knew enough about cryptanalysis to devise an ingenious method for almost automatically determining the letters of a Playfair keyword. In France, however, Moorman did not engage in any actual cryptanalysis, except perhaps to help out, since his work as head of G.2 A.6 was administrative, not operative. As a boss he was well regarded by his men for his fairness and blunt honesty.

G.2 A.6's first real victory in the war of the intercepts came early in 1918 with the shift of the Germans away from the divisional codes that they had long been using—a

series of codes, differing from unit to unit, whose codewords all began with the letters K, R, or U.

It was at midnight of March 11 that the Germans placed into service not merely a new code, but one that, from its numerical codegroups, appeared to be of a different breed entirely. The Allies were expecting a major German push, and the appearance of this code was considered another straw in the wind. Its solution would obviously be of importance in giving clues to German activities. Though the British had suggested that a superencipherment might be involved, the precise nature of the system had to be determined, the superencipherment stripped off, and the repertory then built up. This would have imposed much greater difficulties than just solving another codebook edition—except for American alertness.

Forty minutes after midnight, the American intercept post at Souilly picked up one of the first messages in the new system. Station x2 was sending it to station AN:

00:25 CHi-13 845 422 373 792 240 245 068 652 781 245 659 504

At 12:52 AN replied: CHI-13 os RGV KZD. Five minutes later x2 sent a second message to AN:

00:25 CHI-14 UYC REM KUL RHI KWZ RLF RNQ KRD RVJ UOB KUU UQX UFQ RQK

When these appeared on the desk of code cryptanalyst Lieutenant Hugo Berthold, he guessed at once what had happened: x2 sends a 13-group cipher message (cHi-13) in a new system. AN responds with os, a well-known service abbreviation for *Ohne Sinn* ("message unintelligible"), and a reference to cm-13, followed by two groups from the old KRU code. Whereupon x2 sends a second message, this time in KRU but with the original time group (00:25). The old KRU had been partially solved, and Berthold knew that the RGV of the short AN message meant "old." He did not know the meaning of KZD, but it seemed likely in view of what happened that it meant "Send in code," making the whole phrase "Send in old code." Could the Germans have been so stupid as to compromise their new code within an hour after putting it into service by sending the same message in both the old and the new systems?

Berthold's blue eyes fairly snapped and the few pale wisps of hair that lay against his bald pate almost stood up with excitement as he decoded the second x2 message with his reconstructed KRU. It read:

**UYC REM KUL RHI KWZ RLF RNQ KRD RVJ UOB KUU**

An [?] Bn. 2 h i r sch w

**UQX UFQ RQK**

i tt e

The KWZ and UOB appeared to be nulls, used—almost certainly in violation of regulations—as word dividers, and REM probably meant *Kommandant.* When Berthold checked this against the second message, he saw at once that it had the same plaintext. The repetitions of the plaintext i's and *t's,* which had been masked by the homophones and the lexicon of the KRU code, appeared clearly in the trinumeral message as the repeated 245s and 659s. With these four points as anchors, Berthold could set up the following equivalencies:

845 422 373 792 240 245 068 652 781 245 659 659 504 An [?] Bn. 2 h i r sch w i t t e

A staff airplane sped his result to the British cryptanalytic bureau, and Berthold telegraphed it in a special code-breakers' code to the French. It was a Rosetta Stone for a new forward code called the Schliisselheft. The three bureaus cooperated closely, but it was largely due to a French genius that within two days they had neutralized the Schliisselheft superencipherment and dismembered much of the lexicon. By March 21, when the expected German blow fell, Allied cryptanalysts were reading Schliisselheft messages better than the German code clerks themselves. Theoretically no important information was supposed to be carried in it, because it was intended only for low-level, . front-line communications. But theory succumbed at times of great activity, when the information was most desirable, and the trinumeral messages were laden with valuable nuggets. "The sending of this one message must certainly have cost the lives of thousands of Germans," Moorman said, "and conceivably it changed the result of one of the greatest efforts made by the German armies."

It was also in preparation for this Great German onslaught that another new cipher made its appearance. This was the ADFGVX system, the most famous field cipher in the whole history of cryptology. It was so named because only those six letters occurred in its cryptograms, though just five were used (no v) when the system sprang into use on March 5, 1918.

The war in the West had by then become a stalemate of exhaustion. The young recruits who the Kaiser had promised in the glorious summer of 1914 would be "home before the leaves fall" had become veterans hardened by almost four years of battle—those few who survived. The flower of England's youth had perished; in France, a generation had climbed out of the trenches and vanished forever.

During the winter, Germany had come to realize that she would have to win in the spring if she were to win at all. The U-boat had failed to starve England into submission, and the United States had entered the war against her. But the collapse of Russia had freed dozens of German divisions for service on the Western Front and, for the first time, Germany held a numerical preponderance there. This, however, was only until America could transport her strong young forces across the Atlantic. It was to be now or never, and the imperial government lashed its weary troops and hungry civilians for the supreme effort that was to bring final victory.

It was no less clear to the Allies that Germany planned to launch a climactic offensive in the spring. There were many signs—the new cipher itself was one. The question was: Where and when would the actual blow fall? The German high command, recognizing the incalculable military value of surprise, shrouded its plans in the tightest secrecy. Artillery was brought up in concealment; feints were flung out here and there along the entire front to keep the Allies off balance; the ADFGVX cipher, which had reportedly been chosen from among many candidates by a conference of German cipher specialists, constituted an element in this overall security, as did the new Schliis-selheft. The Allies bent every effort and tapped every source of information to find out the time and place of the real assault. But one of their most flowing founts—cryptanalysis — appeared to have dried up.

When the first ADFGX messages got to Georges Painvin,

the best cryptanalyst in the Bureau du Chiffre, he stared at them, ran a hand through his thick black hair with an air of perplexity, and then set to work. The presence of only five letters immediately suggested a checkerboard. Without much hope, he tried the messages as simple monoalpha-betics; the tests were, as he had expected, negative. He discarded a polyalphabetic checkerboard as too cumbersome, and was left with the hypothesis that the checkerboard substitution had been subjected to a transposition. On this basis he began to work.

Nothing happened. The traffic was too light for him even to determine by frequency counts whether the checkerboard key changed each day, and without this basic information he did not dare to amalgamate the cryptograms of successive days for a concerted assault. Colonel Francois Cartier, head of the Bureau du Chiffre, looked on over his shoulder as he braided and unbraided the letters and . mused sadly, "Poor Painvin. This time I don't think you'll get it." Painvin, goaded, worked harder than before. Meanwhile, Berthold achieved his Schliisselheft entry and Painvin, shifting temporarily to that more fruitful field, completed it. But the enciphered code, used only for trench communications, provided no strategic insights. These would come, if they were to come at all, through solution of the ADFGX, which direction-finding showed was carrying messages between the higher German headquarters, chiefly those of divisions and army corps. Painvin strained even harder.

At 4.30 a.m. March 21, 6,000 guns suddenly fired upon the Allied line at the Somme in the most furious artillery cannonade of the war. Five hours later, 62 German divisions rolled forward on a 40-mile front. The surprise was complete and its success overwhelming. French and British troops reeled back day after day in stunned confusion. The head of intelligence at French G.H.Q. came into the cryp-tologic bureau three days later and told Major E.-A. Soudart, the replacement for ex-chief Marcel Givierge, and Soudart's assistant, Marcel Guitard: "By virtue of my job I am the best informed man in France, and at this moment I no longer know where the Germans are. If We're captured in an hour, it wouldn't surprise me." Within a week the Germans had punched a hole 38 miles deep in the Allied lines, and it was not until the British and French

troops fell back to Amiens that they collected themselves and halted the advance.

The furious advance was reflected in a dramatic upsurge in radio traffic. The first result was disappointment. Pain-vin's frequency counts showed that the checkerboard key did change daily; presumably the transposition key did also. Solution would therefore require a goodly quantity of text from a single day, but until April 1 the interceptions were too meager. On that day, the French picked up 18 ADFGX messages totaling 512 five-letter groups. Two had been sent in three parts, and Painvin noticed on April 4 that the first parts of the two messages had identical bits and pieces of text larded in the same order in the cryptograms. This oddity could most likely have resulted from both cryptograms having identical beginnings transposed accordingly to the same key; the identical fragments of text would then represent the identical tops of the columns of the transposition tableau. Sectioning the cryptograms so that each identical fragment started a new segment would yield the columns of the tableau, in the order of their transcription. Painvin cut up the cryptograms so that each identical fragment started a new segment. These segments constituted the columns of the tableau in the order of their transcription. Painvin then noticed that some columns were long in both cryptograms, some were short in both, and some were long in one and short in the other. The long columns must have stood at the left of the transposition tableau. Those keynumbers must therefore have been the first in the transposition key. Painvin thus made a first approximation to that key. Pursuing this reasoning, he distributed the keynumbers in zones within the key. He then put columns side by side and counted the resultant letter pairs. Most counts were flatfish, displaying no distinctive characteristics. But some appeared monoalphabetic in nature—some highs, some mediums, many blanks. These counts represented two columns that had stood side by side in the original tableau and so contained the digraphic substitutes from the checkerboard. In this way Painvin gradually built up the entire transposition key. When he had done that, he had only to solve the checkerboard substitution as a monoalphabetic to reach the plaintext. After 48 hours of incredible labor, Painvin had cracked the first messages in the toughest field cipher the world had yet seen.

His feat shows the cryptanalytic mind at its finest. Pain-vin spotted opportunities that many would have missed, and when he worked with one, he did not leave it until he had wrung it dry. This technique of extracting every drop of information from each phase of solution before moving on served well, for the cipher prickles with many defenses. From the German point of view, the system was quick and easy, involving only two simple steps. Messages were doubled in length, but this disadvantage was somewhat offset by the presence of only five different letters in the cryptograms, making transmission faster and more accurate. The ADFGX letters of the coordinates had been chosen by the inventor of the system, Lieutenant Fritz Nebel, because he had found them easy to remember when first learning the Morse code.

By the time Painvin had achieved his first solution, the first German offensive had spent its force, and the volume of traffic had diminished. After three weeks of work, he managed on April 26 to achieve his second solution. Meanwhile the Germans again struck with surprise and forced the English back almost to the sea. But Painvin was getting his feet on the ground, and the subsequent key recoveries came with increasing speed: nine and a half days, two days, and, finally, one day.

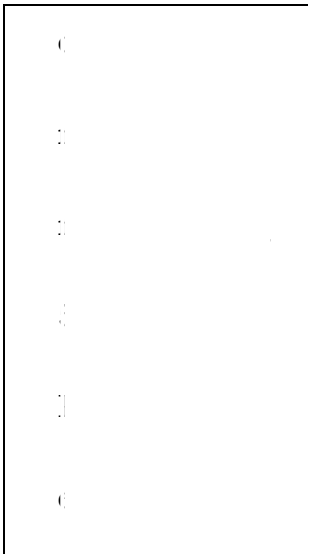
But by then the French had been dealt two unpleasant blows—one military, one cryptographic. Ludendorff had again managed to conceal the time and place of a major assault. Fifteen of his divisions fell by surprise on seven. A gray flood of Germans inundated the French positions in the heights of the Chemra-des-Dames and surged forward irresistibly until it lapped the banks of the Marne only 30 miles from Paris, almost submerging the Allied cause. At the same time, Painvin suddenly saw, on June 1, the ADFGX messages complicated by the addition of a sixth letter, v. Probably the Germans expanded their checkerboard to 6 X 6. But why? For homophones to further blunt the frequency clues? Or to insert the ten digits? Painvin did not know.

"In short," he said, "I had a moment of discouragement. The last two keys of the 28th and the 30th of May had been discovered under conditions of such rapidity that their exploitation was of the greatest usefulness. The offensive and the German advance still continued. It was of the greatest importance not to lose [cryptanalytic] contact and

in my heart I did not want to brusquely shut off this source of information to the interested services of the armies, which had become accustomed to counting on its latest results."

He opened his assault on the cryptograms of June 1 at 5 p.m. Three messages of that date all bore the same time group (00:05) and had all been sent from a transmitter with call-sign GCI. Noticing that a message to call-sign DAX had 106 letters and one to call-sign DTD had a similar text of 108 letters, he assumed that the two plaintexts were the same except for the addition of a single element to the internal address of the DTD message. He had only to seek an arrangement of columns that would produce such a pair of cryptograms. Within an hour he had found it:

6 16 7 5 17 2 14 10 15 9 13 1 21 12 4 8 19 3 11 20 18 The solution of the checkerboard followed quickly:



The DAX plaintext read: *14 ID XX Gen Kdo ersucht vordere Linie sofort drahten XX Gen Kdo 7* ("14th Infantry Division: HQ requests front line [situation] by telegram. HQ 7th [Corps]"). The DTD text was identical except for its being addressed *216 ID.*

Painvin completed his solution at 7 p.m. on June 2, and sent it at once to G.H.Q. By then the French had managed to halt Ludendorff's push, but they teetered precariously on the brink of defeat. The Germans were shelling Paris from 60 miles away with their long-range guns. The great German successes of March and May had driven two vast salients into Allied territory. They pointed like daggers at Paris. And the great question recurred: Where would Ludendorff strike next? The thin Allied lines could not hold against a massive piledriver blow concentrated on a single point. If Ludendorff could gain the same surprise that he had so successfully achieved in each previous assault, he

could puncture the Allied defenses, overrun Paris, and perhaps end the war. The Allies' only hope of stopping him was to absorb his thrust head-on with their reserves. But to do this they had to know where to send them.

The French discussed the possibilities. Would Luden-dorff lunge out directly for Paris from the tip of one of his salients despite the danger to their flanks? Or would he first flatten out the large dent between those bulges and then drive forward from a consolidated position? If the latter, where in the huge pocket would he strike? No one knew.

Ludendorff, meanwhile, was having troubles of his own. German military doctrine called for a sudden, intense artillery bombardment to paralyze the defenders before the infantry attacked. This saturation technique required concentrating thousands of field pieces and tons of munitions at the battle-front. At a conference early in June, Ludendorff learned that this concentration was running behind the schedule he had set for his next assault. His successes had strained his lines of transport, and he had been moving his guns and shells only under cover of night to preserve the invaluable advantage of surprise.

And this advantage he had conserved superbly. The hints that drifted out to French G.H.Q. about his intentions were multiple, petty, and contradictory. Nothing would jell. Gloomy intelligence officers could reach no definite conclusions. Another attack was certainly in the offing, but unless they could ascertain its location, France might be lost.

Into this dismal atmosphere on the morning of June 3 burst Guitard of the Service du Chiffre, excitedly waving an intercept. One of the G.H.Q. cryptanalysts, applying the keys that Painvin had sent there, had just read a cryptogram sent at 4:30 a.m., only a few hours earlier:

**CHI-126 FGAXA XAXFF FAFFA AVDFA GAXFX FAAAG DXGGX AGXFD XGAGX GAVGX AGXVF VXXAG XFDAX GDAAF DGGAF FXGGX XDFAX GXAXV AGXGG DFAGD GXVAX XFXGV FFGGA XDGAX ADVGG A**

Direction-finders reported that it had been transmitted by the German High Command. The addressee, Die, was known from traffic analysis and direction-finding to be the 18th Army's general staff in Remaugies—a town situated just above the concavity in the German lines. Its plaintext

read: *Munitionierung beschleunigen Punkt Soweit nicut* [error for *nichf\ eingesehen auch bei Tag* ("Rush munitions Stop Even by day if not seen").

Guitard and the intelligence officers recognized at once that the ammunition mentioned in the telegram was that intended for the usual German pre-assault bombardment, and the location of the addressee of the message told them where that attack would come. Jubilantly they communicated their information to the operations officers: Ludendorff was going to hammer out the dent, and the German sledge would crash down onto the French line between Montdidier and Compiegne, a sector about 50 miles north of Paris.

Aerial reconnaissance confirmed the daylight transport of munitions. Deserters reported that the onslaught would take place June 7. Foch, in supreme command, shifted his reserves into position, thinned out the front lines, upon which the brunt of the cannonade would fall, and braced his secondary defenses. On the 6th, officers were told that "the offensive is imminent." Tension mounted. The 7th passed without enemy action, and the 8th: Ludendorff had postponed the attack for two days to bring up more guns and munitions because, he said, "thorough preparation was essential to success." The French waited tensely but with confidence. At midnight on June 9 the front from Montdidier to Compiegne erupted in a fierce, pelting hurricane of high-explosive, shrapnel, and gas shells. For three hours a German artillery concentration that averaged one gun for no more than ten yards of front poured a continual stream of fire onto the French positions—and Ludendorff's urgent demand for ammunition became clear. But this time, for the first time since Ludendorff began his stupendous series of triumphs, there was no surprise. Painvin's manna had saved the French.

A little before dawn 15 German divisions charged forward. The French were ready. For five days, fighting seesawed back and forth. Initially the Germans took the little villages of Mery and Courcelles, but on June 11, General Charles Mangin counterattacked with five divisions and all the elan the French could muster. He stopped the German advance cold and then swept the gray tide out of the two villages. Again the Germans heaved forward in a great effort. They failed with heavy losses. For the first time that spring, Ludendorff suspended an operation before it had

achieved its goal. Mangin, wearing his gold-brocaded kepi, laughed beneath the guns of victory. Foch, who realized that other German assaults would come and that he would have to defend against them, knew at last that he would some day take the offensive. He knew then that the war was not lost, and could eventually be won. Within a few weeks, the final German thrusts did come, but they had run out of steam, and the French parried them. Soon the initiative passed to the Allies, bolstered by the Americans, and their powerful counterstrokes drove the German armies back and back until the Kaiser, his militaristic dreams wrecked, abdicated and fled while his generals signed the Armistice at Compiegne. The World War was ended.

For Painvin, who had lost 33 pounds while simply seated at his desk, there was a long leave of convalescence. Afterwards, he engaged in an immensely successful business career, becoming president and director general of Ugine, the chemical giant of France, president of a phosphate company, vice president of a commercial credit firm, administrator of a mortgage society, honorary president of the Union of Chemical Industries and of the central committee of the electrochemical trade, and president of the Chamber of Commerce of Paris. Yet, he said, none of these achievements ever gave him the satisfaction that his ADFGVX solutions did. They left "an indelible mark on my spirit, and remain for me one of the brightest and most outstanding memories of my existence."

The First World War marks the great turning point in the history of cryptology. Before, it was a small field; afterwards, it was big. Before, it was a science in its youth; afterwards, it had matured. The direct cause of this development was the vast increase in radio communications.

This heavy traffic meant that probably the richest source of intelligence flowed in these easily accessible channels. All that was necessary was to crack the protective sheath. As cryptanalysis repeatedly demonstrated its abilities and worth, it rose from an auxiliary to a primary source of information about the foe; its advocates spoke regularly in the councils of war. The emergence of cryptanalysis as a permanent major element of intelligence was the most striking characteristic of cryptology's new maturity.

Another was the change in cryptanalysis itself. The science at last outgrew the mode of operation that had

1

dominated it for 400 years. This was chamber analysis, in which a single man wrestles with a single cryptogram alone in his room; Rossignol epitomizes the genre. As cipher systems grew increasingly complex, cryptanalysts relied more and more on special solutions, and so they required many more messages for success than the bewigged practitioners of chamber analysis would have ever thought necessary.

A third characteristic of the new maturity was the evolution of fields of cryptanalytic specialization. Systems of secret communication had ceased to be so few and so homogeneous that a single expert could subdue them all. Their multiplicity and heterogeneity, plus the volume of traffic in each, bred the specialist. This division of labor is as much a sign of maturity in cryptology as it is in a society.

Still another sign of that maturity was the emotional apprehension of the role played by the blunders of inexperienced, indolent, and ignorant cryptographic clerks. Cryptologists had had an intellectual awareness of this danger at least since 1605, when Francis Bacon wrote that "in regards of the rawness and unskillfulnesse of the handes, through which they passe, the greatest Matters, are many times carryed in the weakest Cyphars." But it was not until cipher key after cipher key, and code after code, had been betrayed by needless mistakes or stupidities or outright rule violations that the magnitude of the problem was borne in upon them. The problem had swollen to such proportions because so large a volume of messages had to be handled by so many untrained men—against whom were pitted the best brains of the enemy. The experts realized that to eliminate these is to strengthen cryptographic security more effectively than by introducing the most ingenious cipher. The great practical lesson of World War I cryptology was the necessity of infusing an iron discipline in the cryptographic personnel.

All these developments, however, resulted essentially from the interreaction between cryptology and the outside world; they were externally oriented. World War I originated no developments that were internally oriented, as, for example, was the emergence of the field cipher. On the contrary, two of the most central activities—the actual cryptographic operations, which were performed by hand, and the techniques of solution, which were brute frequency analysis—had exhausted their usefulness. Manual systems sagged under message loads for which

they were never designed. Not a few cryptographic clerks dreamed of machines that would lift the onerous burden from their shoulders. In a sense, the codes that became so popular might be regarded as a rudimentary form of mechanical device that does the work for the encoder: the phrases are prepared and equated with their code equivalents in advance, and the encoder has but to pick out the ones he wants. But the trench codes were to the printing cipher machines of later years as the taxis of the Marne were to the armored troop-carriers of Panzer columns.

At the same time, the classic principles of frequency analysis had been stretched to their utmost. They were applied with great subtlety, as in Painvin's solving the ADFGVX transposition. But no new principles had been evolved, and the old ones had barely coped with such concepts as fractionation.

In these two internal matters, which lie at the core of cryptology, World War I marked not the beginning but an end, had reaped not fulfillment but barrenness. So viable had the science become, however, that this very vacuum, this want, held promise.

## 10. Two Americans

THE MOST FAMOUS CRYPTOLOGIST in history owes his fame less to what he did than to what he said—and to the sensational way in which he said it. And this was most perfectly in character, for Herbert Osborne Yardley was perhaps the most engaging, articulate, and technicolored personality in the business.

He was born April 13, 1889, in Worthington, Indiana, and grew up in that little Midwestern town during the tranquil, sunlit years that preceded the First World War. A popular youngster, he was president of his high-school class, editor of the school paper, and captain of the football team, and though only an average student, he had a flair for mathematics. From 16 on he frequented the poker tables of the local saloons, learning the game that was to be a passion of his life. He had wanted to become a criminal

I

lawyer, but instead landed at 23 as a $900-a-year code clerk in the State Department.

It was a case of purest serendipity, for the man and the subject were ideally matched. His romantic mind thrilled to the stream of history that daily poured through his hands in the form of ambassadorial dispatches, and cryp-tology fired his imagination. He had heard vague tales of cryptanalysts who could pry into secrets of state, and when a 500-word message from Colonel House passed over the wires to President Wilson one night, Yardley, with characteristic audacity, determined to see whether he could solve what must be the most difficult of American codes. He astonished himself by solving it in a few hours.* His success cemented his attachment to cryptanalysis, and he followed this demonstration of the low estate of high-level cryptography with a 100-page memorandum on the solution of American diplomatic codes. While absorbed in possible solutions for a proposed new coding method, he diagnosed what has ever since been known among cryptol-ogists as the "Yardley symptom": "It was the first thing I thought of when I awakened, the last when I fell asleep."

Soon after the American declaration of war in April of 1917, he sold the idea of a cryptologic service to the War Department. He succeeded partly because the need was genuine, partly because he himself was an exceedingly convincing young man. Yardley had proven his cryptanalytic ability, and moreover had done well enough in his regular duties to have won raises to $1,400 in 43 months. Major Ralph H. Van Deman, later to be known as the Father of American Intelligence, commissioned the thin, balding 27-year-old as a lieutenant and set him up as the head of the newly created cryptologic section of the Military Intelligence Division, MI-8.

*The President and his advisor were then using two main systems. One was external—a superencipherment applied to the five-digit numerical groups of what probably was a State Department code. The first digit was enciphered by one of two alternate letters; the two pairs by a vowel-consonant combination. Thus, in one edition of the superencipherment, 40606 became FEDED, 40699, KEDIR, and so on. The other was internal—a jargon code of such less-than-Stygian incognitos as MASS for the Secretary of War, NEPTUNE for the Secretary of the Navy, BLUEFIELDS for William C. Redfield, Secretary of Commerce, ALLEY for Franklin K. Lane, Secretary of the Interior, and MANSION for David F. Houston, Secretary of Agriculture. Yard-ley does not specify which he solved.

Like Topsy, MI-8 just grew. First to arrive, to take charge of the instruction subsection for training A.E.F. cryptanalysts, was Dr. John M. Manly, a 52-year-old philologist who headed the Department of English at the University of Chicago and was later president of the Modern Language Association; a longtime hobbyist in cryptology, he was to become Yardley's chief assistant and one of his best cryptanalysts. Manly brought with him a bevy of Ph.D.'s clanking with Phi Beta Kappa keys, mostly from the University of Chicago.

The instruction subsection did its teaching at the Army War College. It advanced far enough to offer as Problem 20 "General Principles of attack on enciphered code when the book is known but the system of encipherment unknown." Another subsection popped into being for code and cipher compilation; it produced a military intelligence code, two geographical codes for combat information from France, and a casualty code, which was never used. Soon a communications subsection was handling close to 50,000 words a week. As the organization expanded, it shifted to ever-larger quarters. Beginning in the balcony overhanging the library of the War College, MI-8 moved to the Colonial, an apartment house at 15th and M Streets barely ready for occupancy, and then to a building on the site of what is now the Capitol Theatre on F Street, all in Washington. For security, its offices were always on the top floor.

Growth continued apace. An intercepted letter in a German shorthand instigated a shorthand subsection that soon could read missives in more than 30 systems, most commonly Gabelsberger, Schrey, Stolze-Schrey, Marti, Brock-away, Duployee, Sloan-Duployan, and Orillana. A blank piece -ef paper discovered in the shoe heel of a woman suspected of working with German espionage in Mexico turned out to bear a message in invisible ink. Fortunately, it proved one of the simpler kinds, which can be developed by heat. But it sparked the establishment of a secret-ink subsection whose expert chemists could detect writing in an invisible ink disguised as a perfume with an actual odor and with only one part in 10,000 of solid matter.

The Germans later replaced inks in so bulky and conspicuous a form as liquids with chemicals that were impregnated into scarves, socks, and other garments. They had only to be dipped in water to create the writing fluid. These miracles of the test tube, called F and P inks by the

I

British chemists who taught the Americans much of what they knew, were so precisely formulated that they would react with only one other chemical to form a visible compound.

Eventually, the Allied chemists discovered a reagent that brought out secret writing in any kind of ink, even clear water. Crystals of iodine, heated gently, sublimated into fumes of a beautiful violet hue that settled more densely in those fibers of paper that had been disturbed by any kind of wetting action, thus tracing the pen's course. The Germans replied by writing in a sympathetic ink and then moistening the entire sheet. The Allies struck back with a chemical streak test that would show whether the paper surface had been dampened. This was almost as incriminating as actual development of a secret-ink letter, for who but a spy would wet a letter? The seesaw battle between the chemists of Germany, traditionally world leaders in that science, and those of the Allies reached a stalemate when both sides discovered the general reagent—one that would develop any secret ink at any time, even on moistened paper. Formulas differ slightly, but all use a mixture of iodine, potassium iodide, glycerine, and water, dabbed on with cotton. The liquid concentrates in the more disturbed fibers and reveals the writing. By the time this general reagent appeared, MI-8's secret-ink subsection was testing 2,000 letters a week for invisible writing and had discovered 50 of major importance. Among them were letters that led to the capture of Maria de Victoria, a beautiful German spy who was planning to import high explosives for sabotage inside the hollow figures of saints and the Virgin Mary!

MI-8 also solved cryptograms. It read diplomatic telegrams of Argentina, Brazil, Chile, Costa Rica, Cuba, Germany, Mexico, Spain, and Panama. The Spanish-language texts constituted the bulk of its cryptanalytic work. The censorship office sent over intercepted cipher letters; most of these turned out to be merely personal notes in very simple systems, though some of the love letters were so torrid that Yardley said, "It rather worried me to see husbands and wives trust their illicit correspondence to such unsafe methods."

Perhaps the most important of the MI-8 solutions was the one that largely resulted in the conviction of the only German spy condemned to death in the United States dur-

ing World War I. This was Lothar Witzke, alias Pablo Waberski, who was suspected of setting off the Black Tom explosion. He was captured in January, 1918, by an American agent, who found in his baggage in the Central Hotel in Nogales, Mexico, a cipher letter dated January 15. It did not reach MI-8 until spring, and then it kicked about for a few more months while several men there tried and failed to solve it. Finally Manly took it up.

This quiet scholar, who never married and whose quiet, simple manner contrasted so sharply with his chief's, was to become one of the world's leading authorities on Chaucer. He and his collaborator, Edith Rickert, labored for 14 years to produce their monumental eight-volume work, *The Text of the Canterbury Tales,* in which, by a tedious collation of scribal errors and variant readings in more than 80 manuscripts of the medieval masterpiece, they reconstructed a text that is as close to the poet's own original as the extant evidence allows. The cast of mind that can thus sort out, retain, and then organize innumerable details into a cohesive whole was just what was needed for the Gothic complexity of the 424-letter Witzke cryptogram. In a three-day marathon of cryptanalysis, Manly, aided by Miss Rickert, perceived the pattern of this 12-step official transposition cipher, with its multiple horizontal shiftings of three- and four-letter plaintext groups ripped apart by a final vertical transcription. He drew forth a message from Heinrich von Eckardt, the luckless German minister in Mexico whose very involvement with a cryptogram seemed to mean its cryptanalysis,* to the German consular authorities:

"The bearer of this is a subject of the Empire who travels as a Russian under the name of Pablo Waberski. He is a German secret agent. Please furnish him on request protection and assistance; also advance him on demand up to 1,000 pesos of Mexican gold and send his code telegrams to this embassy as official consular dispatches." When Manly read this to a military commission of colonels and generals who were trying Witzke on spy charges in a hushed courtroom at Fort Sam Houston,

*In addition to this and the Zimmermann telegram, two messages to the diplomat from his home office, encoded in the English-French half of Clifton's *Nouveau Dictionnaire Frangals,* which had replaced the betrayed Cipher 13040, were solved by MI-8. They disclosed Germany trying to bribe Mexico to remain neutral.

San Antonio, the effect was condemnatory. The handsome young spy was sentenced to death. Wilson later commuted it to life imprisonment, however, and Witzke was released in 1923.

In August of 1918, Yardley sailed for Europe to learn as much as he could from America's allies. He obtained entrance to Great Britain's M.I. l(b) after demonstrating his abilities and there studied British methods for the solution of different codes and ciphers. The doors of Room 40 remained resolutely locked against him as against everyone else, though Hall did give him a German naval code and a neutral nation's diplomatic codes. In Paris that fall, Yardley met Painvin, who gave him a desk in his office and invited him to his home many evenings. But he never gained access to the French Foreign Ministry crypt-analytic bureau.

He remained in Paris after the Armistice to head the cryptologic bureau of the American delegation to the Peace Conference. At first there was a tremendous rush to get organized, but then the pressure eased, and Yardley and helpers Lieutenants J. Rives Childs of G.2 A.6 and Frederick Livesey, who had been sent over from MI-8, enjoyed the life of playboy cryptologists. A practical soul, Yardley saw no need for the three officers assigned to the bureau to be present at once, and so a rotation of duties was arranged that permitted them to spend most of their time at the international cocktail parties and dancings that were then the rage of Paris.

When it ended, as it had to, Yardley, viewing with distaste a return to the State Department code room, and burning with evangelical fervor over America's need for cryptanalysis, exercised his potent salesmanship on the State and War departments. He won the concurrence of Frank L. Polk, the acting Secretary of State; then, on May 16, 1919, he submitted to the Chief of Staff a plan for a "permanent organization for code and cipher investigation and attack." Three days later the Chief of Staff approved it, and Polk brown-penciled an "O.K." and his initials on it. The plan envisioned joint financial support by the two departments at about $100,000 a year, but actual expenditures never reached that sum. The State Department's contribution of $40,000, which began on July 15, 1919, could not be legally expended within the District of Columbia, and so Yardley soon found himself

moving the nucleus of a staff (largely recruited from MI-8) and the necessary paraphernalia—language statistics, maps, newspaper clipping, dictionaries—to New York City.

By October 1 the organization that was to become known as the American Black Chamber was ensconced in the former town house of T. Suffern Tailer, a New York society man and political leader, at 3 East 38th Street. It stayed there little more than a year, however, before moving to new quarters in a four-story brownstone at 141 East 37th Street, just east of Lexington Avenue. It occupied half of the ornate, divided structure, whose high ceilings did little to relieve the claustrophobic construction of its twelve-foot-wide rooms. Yardley's apartment was on the top floor. All external connection with the government was cut. Rent, heat, office supplies, light, Yardley's salary of $7,500 a year, and the salaries of his staff were paid from secret funds. Though the office was a branch of the Military Intelligence Division, War Department payments did not begin until June 30, 1921.

One of the organization's first assignments was to solve the codes of Japan, with whom friction had been growing. Yardley, in an access of enthusiasm, promised the solution or his resignation within the year. He regretted his impetuousness as soon as he plunged into the task, for he almost foundered in the Oriental intricacies of Japanese plaintext, to say nothing of codetext. After some preliminary study, assisted by Livesey, who had a great aptitude for languages, he ascertained that the Japanese employed a watered-down form of their ideographic writing called "kata kana" for telegraphic and—presumably— cryptologic communication, which was transmitted in Latin letters. Kata kana consists of about 73 syllables, each with a sign of its own which had been given a roman equivalent, and when Yardley had his typists compile frequency tables for the twenty-five plain-language kata kana telegrams he had, he discovered that this script obeyed rules of frequency just like any other. Specifically, the kana *n,* the only nonsyllabic kana, was most common, appearing often at the end of words, followed by *i, no, o, ni, shi, wa, ru,* and *to,* in that order. The list of most common syllables and words began with *ari* and continued with *aritashi, daijin, denpoo, gai, gyoo,* and so on. At the end of about four months, the typists had prepared elaborate

I

statistics ot frequency and contact for about 10,000 kana. He then set them to work dividing the ten-letter groups of the Japanese code telegrams into pairs of letters and drawing up similar frequency and contact data for these pairs. He himself went through the approximately 100 code telegrams underlining with colored pencils all repetitions of four letters or more. But despite the most intensive scrutiny and study, no solution was forthcoming. Livesey's linguistic abilities had meanwhile brought him a fair acquaintance with Japanese. He found in a bilingual dictionary that he had bought for 75 cents that the word *owari* meant "conclusion." Could it be the plaintext of certain codegroups found frequently at the end of telegrams? The hypothesis, involving only three kana, proved barren. He examined the plain-language telegrams and pointed out probable words with conspicuous patterns to Yardley. Two of these, which played a vital role in the solution, were "Airurando do-kuritsu" ("Ireland independence"), with the repeated *do,* and "Doitsu" ("Germany"), which used three of the same kana in a different order. This was a good clue, but it alone was not the answer. Night after night Yardley would climb the stairs to his apartment, weary, hopeless, discouraged, and fall into bed, only to wake up excitedly a few hours later with a brilliant idea—which invariably turned out to be just another blind alley.

> By now [he wrote] I had worked so long with these code telegrams that every telegram, every line, even every code word was indelibly printed in my brain. I could lie awake in bed and in the darkness make my investigations—trial and error, trial and error, over and over again.
>
> Finally one night I awakened at midnight, for I had retired early, and out of the darkness came the conviction that a certain series of two-letter codewords absolutely *must* equal *Airurando* (Ireland). Then other words danced before me in rapid succession: *dokuritsu* (independence), *Doitsu* (Germany) , *owari* (stop). At last the great discovery! My heart stood still, and I dared not move. Was I dreaming? Was I awake? Was I losing my mind? A solution? At last—and after all these months!
>
> I slipped out of bed and in my eagerness, for I knew I was awake now, I almost fell down the stairs.

With trembling fingers I spun the dial and opened the safe. I grabbed my file of papers and rapidly began to make notes.

These promptly proved his intuitions correct. The repetitions of RE for *do,* BO for *tsu,* OK for *ri,* and UB for i in his equivalences confirmed it:

WI UB PO MO IL KB  RE OS OK BO  RE UB BO  AS FT OK

a  i  ru ra  n  do  do ku  ri tsu  do  i  tsu  o  wa ri

For an hour Yardley filled in these and other identifications and then, convinced that the opening wedge had been driven, went upstairs, awoke his wife, and went out to get drunk. Actually, considerably more work had to be done before the Black Chamber could read anything approaching sentences. Much of this was done by Livesey, who achieved an important secondary breakthrough when he identified the Japanese plaintext *jooin* ("Senate") and *jooyakuan* ("draft treaty").

Yardley encountered unexpected difficulties in finding a translator for the exotic language, but finally located a kindly, bewhiskered missionary. He looked jokingly incongruous in the Black Chamber, but he enabled Yardley to send the first translations of Japanese telegrams to Washington in February of 1920. He quit after six months when he finally realized the espionage nature of the work, but by then Livesey had accomplished the almost unheard-of feat of learning Japanese in that time.

Yardley called the first code "Ja," the "J" for Japanese, the "a" a serial for the first solution. From 1919 to the spring of 1920 the Japanese introduced eleven different codes, having employed a Polish expert, Captain Kowalef-sky, to revise then" cryptologic systems. Kowalefsky taught the Japanese how to bi-, tri-, and tetrasect their messages: to divide them into two, three, or four parts, shuffle the parts, and then encipher them in transposed order to bury stereotyped beginnings and endings. Some of the codes contained 25,000 code groups.

During the summer of 1921, the Black Chamber solved telegram 813 of July 5 from the Japanese ambassador in London to Tokyo. It contained the first hints of a conference for naval disarmament—an idea that powerfully gripped the imagination of a war-weary world. Another indication came when Japan suddenly introduced a new

code, the YU, for their most secret messages. On solution, it was dubbed "Jp"—the sixteenth solved since Yardley's original break.

A few months before the November opening of the disarmament conference in Washington, daily courier service was set up between the Black Chamber and the State Department. An official grinningly remarked that State's upper echelons were delighted with the cryptanalysts' work and read the solutions every morning with their orange juice and coffee. The conference sought to limit the tonnage of capital ships, and as negotiations were proceeding toward its chief result—the Five-Power Treaty that accorded tonnages in certain ratios to the United States, Britain, France, Italy, and Japan—Yardley's team was reading the secret instructions of the negotiators. "The Black Chamber, bolted, hidden, guarded, sees all, hears all," he wrote later, rather melodramatically. "Though the blinds are drawn and the windows heavily curtained, its far-seeking eyes penetrate the secret conference chambers at Washington, Tokyo, London, Paris, Geneva, Rome. Its sensitive ears catch the faintest whisperings in the foreign capitals of the world."

Each nation naturally tried to obtain the most favorable tonnage ratio for itself; the most aggressive in its efforts was Japan, which even then was dreaming expansionist dreams in Asia but feared to offend the United States. At the height of the conference, when Japan was demanding a ratio of 10 to 7 with the United States and Great Britain, the Black Chamber read what Yardley later called the most important telegram it ever solved.

"It is necessary to avoid any clash with Great Britain and America, particularly America, in regard to the armament limitation question," the Japanese Foreign Office cabled its ambassador in Washington on November 28. "You will to the utmost maintain a middle attitude and redouble your efforts to carry out our policy. In case of inevitable necessity you will work to establish your second proposal of 10 to 6.5. If, in spite of your utmost efforts, it becomes necessary in view of the situation and in the interests of general policy to fall back on your proposal No. 3, you will endeavor to limit the power of concentration and maneuver of the Pacific by a guarantee to reduce or at least to maintain the status quo of Pacific defenses and to make an adequate reservation which will

make clear that [this is] our intention in agreeing to a 10 to 6 ratio. No 4 is to be avoided as far as possible."

Each 0.5 in the ratio meant 50,000 tons of capital ships, or about a battle ship and a half. With the information in this message telling the American negotiators that Japan would yield if pressed, all they had to do was press. This Secretary of State Charles Evans Hughes did, and on December 10 Japan capitulated, instructing its negotiator, in a cable read by the Black Chamber, that "there is nothing to do but accept the ratio proposed by the United States." As signed, the Five-Power Treaty allotted capital ships to the United States, Great Britain, Japan, France, and Italy in the ratio of 10:10:6:3.3:3.3. It was considerably less than Japan had hoped for. Hughes sent Yardley a letter of commendation.

During the conference, the Black Chamber had turned out more than 5,000 solutions and translations. Yardley nearly suffered a nervous breakdown, and in February went to Arizona for four months to recover his health. Several of his assistants had already had trouble in this regard. One babbled incoherently; a girl dreamed of chasing around the bedroom a bulldog that, when caught, had "code" written on its side; another could lighten the enormous sack of pebbles that she carried in a recurring nightmare only by finding a stone along a lonely beach that exactly matched one of her pebbles, which she could then cast into the sea. All three resigned.

Yardley's appropriation had been severely cut in 1924, and half the staff had to be let go, reducing the force to about a dozen. Despite this, Yardley said, the Black Chamber managed to solve, from 1917 to 1929, more than 45,000 telegrams, involving the codes of Argentina, Brazil, Chile, China, Costa Rica, Cuba, England, France, Germany, Japan, Liberia, Mexico, Nicaragua, Panama, Peru, San Salvador, Santo Domingo (later the Dominican Republic) the Soviet Union, and Spain and made preliminary analyses of many other codes, including those of the Vatican.

Suddenly it all ended. Yardley, who had been obtaining the code telegrams of foreign governments through the cooperation of the presidents of the Western Union Telegraph Company and the Postal Telegraph Company, was encountering increasing resistance from them. Herbert Hoover had just been inaugurated, and Yardley resolved

I

to settle the matter with the new administration once and for all. He decided on the bold stroke of drawing up "a memorandum to be presented directly to the President, outlining the history and activities of the Black Chamber, and the necessary steps that must be taken if the Government had hoped to take full advantage of the skill of its cryptographers." He waited to see which way the wind was blowing before making his move—and found that it was not with him. Yardley went to a speakeasy to listen to Hoover's first speech as President and sensed, in the high ethical strictures that Hoover expressed, the doom of the Black Chamber.

He was right, though its actual closing came from elsewhere. After Henry L. Stimson, Hoover's Secretary of State, had been in office the few months that Yardley thought would be necessary for him to have lost some of his innocence in wrestling with the hardheaded realities of diplomacy, the Black Chamber sent him the solution of an important series of messages. But Stimson was different from previous Secretaries of State, on whom this tactic had always worked. He was shocked to learn of the existence of the Black Chamber, and totally disapproved of it. He regarded it as a low, snooping activity, a sneaking, spying, keyhole-peering kind of dirty business, a violation of the principle of mutual trust upon which he conducted both his personal affairs and his foreign policy. All of this it is, and Stimson rejected the view that such means justified even patriotic ends. He held to the conviction that his country should do what is right, and, as he said later, "Gentlemen do not read each other's mail." In an act of pure moral courage, Stimson, affirming principle over expediency, withdrew all State Department funds from the support of the Black Chamber.* Since these constituted its major income, their loss shuttered the office. Hoover's speech had warned Yardley that an appeal would be fruitless. There was nothing to do but close up shop. An unexpended $6,666.66 and the organization's files reverted to

*In 1940, as Secretary of War, he had to reverse himself and accept the cryptanalyses of MAGIC. But the international situation then was totally different. "In 1929," he himself has written, in the third person, "the world was striving with good will for lasting peace, and in this effort all the nations were parties. Stimson, as Secretary of State, was dealing as a gentleman with the gentlemen sent as ambassadors and ministers from friendly nations. ..." In 1940, Europe was at war, and the United States was on the verge.

the Signal Corps, where William Friedman had charge of cryptology. The staff quickly dispersed (none went to the Army), and when the books were closed on October 31, 1929, the American Black Chamber had perished. It had cost the State Department $230,404 and the War Department $98,808.49—just under a third of a million dollars for a decade of cryptanalyis.

Yardley, whose job experience had been rather specialized, could not find work, and he went back home to Worthington. The Depression sucked him dry. By August of 1930, he had had to give up an apartment house and a one-eighth interest in a real estate corporation; indeed, he complained that he had to sell nearly everything he owned "for less than nothing." A few months later he was toying with the idea of writing the story of the Black Chamber to make some money to feed his wife and their son, Jack. When his old MI-8 friend, Manly, with whom he had been in contact all during the 1920's, had to turn down his request for a $2,500 loan at the end of January, 1931, Yardley, in desperation, sat down to write what was to be the most famous book on cryptology ever published. He described the composition of it in a letter to Manly in the spring of 1931:

> I hadn't done any real work for so long that I told Bye, my agent, and the Sat Eve Post that I would need some one else to write the stuff. I showed a few things to Bye and Costain, the latter editor of POST, and both told me to go to work myself. I sat for days before a typewriter, helpless. Oh, I pecked away a bit, and gradually under the encouragement of Bye I got a bit of confidence. Then Bobbs Merrill advanced me $1000 on outline. Then there was a call to rush the book. I began to work in shifts, working a few hours, sleeping a few hours, going out of my room only to buy some eggs, bread, coffee and cans of tomatoe juice. Jesus, the stuff I turned out. Sometimes only a thousand words, but often as many as 10,000 a day. As the chapters appeared I took them to Bye who read them and offered criticism. Anyway I completed the book and boiled down parts of it for the articles all in 7 weeks.

The Bobbs-Merrill Company, of Indianapolis, published the 375-page book on June 1, but parts of it had already appeared in three articles at two-week intervals in *The Saturday Evening Post,* the leading magazine of the day, which thought so highly of them that it used the first of the series to lead its April 4 issue. Yardley was a superb storyteller, and his narrative skill did not desert him on paper. Largely owing to this and to his vigorous and pungent style, the book itself, *The American Black Chamber,* was an immediate success, and it instantly fixed itself in popular lore as the epitome of books on cryptology. Even today, it is invariably mentioned in any cocktail-party discussion of the subject, and copies remain in demand among secondhand book dealers. Reviews of it were unanimously good. Critic W. A. Roberts, in a commendatory review, summed up the prevailing opinion: "I think it the most sensational contribution to the secret history of the war, as well as the immediate post-war period, Which has yet been written by an American. Its deliberate indiscretions exceed any to be found in the recent memoirs of European secret agents." Reporters hastened to governmental bureaus to inquire whether it was all true. The State Department, with masterfully diplomatic double-talk, was "disposed to discredit" Yardley's statements. At the War Department, officials lied straightforwardly and said that no such organization had been in existence in the past four years.

Because of these "deliberate indiscretions," *The American Black Chamber* sold 17,931 copies, unprecedented for a book dealing with cryptology, and a highly respectable figure even today. The English edition, entitled *Secret Service in America,* sold 5,480 more. The book was published in French, in Swedish, and in an unauthorized Chinese version, but it was in Japan, as might be expected, that sales skyrocketed. On a per-capita basis, Japanese sales of 33,119 copies were almost four times better than in the United States, where it stirred a tremendous furor. On November 5, Ambassador W. Cameron Forbes reported to the State Department, which had asked "to be kept fully informed" about the Yardley agitation, that "The 'Black Chamber' evidently made a great impression in Japan. I often hear reference made to it in conversation with various classes of Japanese. According to the publishers of the Japanese edition, more than 40,000 copies

have been sold. It remains a best seller at the present time." Contrary to some published reports, however, it did not cause the government to fall (Would that books on cryp-tology were that powerful!), nor Japan to lodge protests with the United States or repudiate the Five-Power Treaty three years later. It did cause Japan to start treating American naval officers there to study the language with suspicion. It did impress itself so indelibly on the Japanese conscience that, when Shigenori Togo became foreign minister ten years later, he recalled the episode and checked to see whether Japanese communications were then secure. And it contributed to anti-American and antiwhite feeling in Japan.

Consequently, when Stanley K. Hornbeck, a Far Eastern expert in the Department of State, heard that Yardley had written a new book, entitled "Japanese Diplomatic Secrets," revealing many Japanese telegrams sent during the 1922 naval disarmament conference, he wrote in a memorandum of September 12, 1932: "I cannot too strongly urge that, in view of the state of excitement which apparently prevails in Japanese public opinion now, characterized by fear of or enmity toward the United States, every possible effort should be made to prevent the appearance of this book. Its appearance would contribute substantially to the amount of explosive material which seems to be piling up in Japan." Apparently as a result of this, United States marshals seized the manuscript on February 20, 1933, at the offices of The Macmillan Company, to whom Yardley had submitted it after Bobbs-Merrill had declined it, on the grounds that it violated a statute prohibiting agents of the United States government from appropriating secret documents.

He tried writing again, but his imagination seemed to need fact to work on, and his adventure novels, *The Red Sun of Nippon* and *The Blonde Countess,* lacked the excitement of his rather fictionalized nonfiction. Metro-Goldwyn-Mayer, however, found the beautiful woman spy, the secret codes, and the infallible cryptologist of *The Blonde Countess* eminently suitable for its purposes. A problem was that no redblooded movie hero would settle for a dull desk job like codebreaking, but the film company fixed that up by destroying the fabric of Yardley's tale and making the hero an unwilling intellectual who wanted only to serve in the trenches overseas. The result was *Rendez-*

*vous,* starring William Powell, Rosalind Russell, Binnie Barnes, Cesar Romero, and Lionel Atwill. Yardley was retained by MGM on a generous contract as technical advisor and became friendly with Powell. The film premiered at New York's Capitol Theatre on October 25, 1935. *The New York Times* reviewed it as a "lively and amusing melodrama."

In 1938, after a brief and unsuccessful fling at real-estate speculation in Queens, New York, Yardley was hired by Chiang Kai-shek at about $10,000 a year to solve the messages of the Japanese armies then invading China. In Chungking, he at first passed himself off as an exporter of hides, but no one in the small and tight-knit foreign colony there was fooled for very long. He seems to have enjoyed some success in solving the Japanese ciphers, which appear to have been columnar transposition of the kana symbols.

By then he was changing. He was basically an attractive personality who enjoyed simple masculine pleasures. He would rise at dawn to go duckhunting, shot a good enough game of golf to have won the Greene County (Indiana) championship in 1932, and played poker with a compulsive intensity wherever and whenever he could. He regaled his companions with a flood of amusing stories, told with the wit and gusto of a natural raconteur. He was the very opposite of stuffy, and did not hesitate to admit that he knew his way around in a Chinese whorehouse. He kept a Chinese and a German mistress* and once organized a virtual Oriental orgy for a young correspondent, later nationally famous, on the ground that it was necessary for him to be blooded as a man. He enjoyed the loyalty and friendship of a great many people, though not everybody liked him. Emily Hahn, in her *China to Me,* said bluntly that she did not, calling him "an American with a loud manner of talking." His original enterprise, which had enabled him to create MI-8 and the Black Chamber, had turned to opportunism with the publication of his book, and then had soured to cynicism under the widespread disgust that followed that violation of confidence, and under the realization that he had traded his soul for a few thousand dollars.

He returned from China in 1940, and, after a brief at-

*At different times.

tempt to be a restaurateur in Washington, went to Canada to set up a cryptanalytic bureau which dealt largely with spy ciphers. He was reportedly forced out under pressure either from Stimson, then Secretary of War, or from the British, though the Canadians did not want to part with him. From 1941 to the end of the war he served as an enforcement officer in the food division of the Office of Price Administration. His popular *The Education of a Poker Player,* in which he offered an informal course of instruction in the game, appeared in 1957. On August 7, 1958, he died of a stroke at his home in Silver Spring, Maryland, and was buried with military honors in Arlington National Cemetery.

The obituaries called him "the father of American cryptography." They were wrong, but they demonstrated the deep impression that Yardley's writing had made on the American consciousness. With all its faults and falsehoods, his book had captured the imagination of the public and inspired untold numbers of amateurs to become interested in cryptology. To the extent that the impact of their fresh ideas enriched American cryptology, the credit must go to him.

While Herbert Yardley may be the best known cryptologist, uncontestably the greatest is William Frederick Friedman. Unlike his contemporary, his eminence is due most emphatically to what he did. Indeed, two more dissimilar men in a single field can scarcely be imagined. Where Yardley was Rabelaisian, outgoing, superficial, free and easy with the details of a good story, and ever ready for the main chance, Friedman tended toward introversion, depth of study, personal security, timidity, dedication, and accuracy, nicety, and validity of work. Despite the relative drabness of these personal traits—or perhaps because of them, Friedman's theoretical contributions and his practical attainments exceed those of any other cryptologist. Yardley's career was like an amazing skyrocket that explodes in fantastic patterns against the heavens. Friedman's was like the sun.

He was born Wolfe Friedman on September 24, 1891, in Kishinev, Russia, the oldest son and second child of Frederick and Rosa Friedman. His father, a Rumanian who spoke eight languages and worked as an interpreter for the Russian Post Office, emigrated to America in 1892, at

which time his son's name was changed to William. The family settled in Pittsburgh, where his father managed a sewing machine agency. William graduated in 1909 as one of the ten honor students in a class of 300 at Pittsburgh Central High School; he then went to work as chief clerk in the Erie City Iron Works, a firm that sold steam engines. About that time the back-to-the-farm movement called to city boys, and in the fall of 1910, Friedman and three friends enrolled in Michigan Agricultural College, whose chief attraction was that it was tuition-free.

But Friedman soon discovered that farming held little interest for him. He was an inventive young fellow who liked to fix things and had written some science fiction for his high-school paper; he was rapidly coming to the conclusion that he liked science. At the end of the term he learned that tuition was also free in a scientific field allied to agriculture—genetics—at one of the Ivy League universities, Cornell. He borrowed train fare and arrived in Ithaca, New York, in February, 1911, where he got a job waiting on tables. After commencement in February of 1914, he attended graduate school, managing to fall in love twice, once with a brunette, once with the blonde daughter of a movie-house owner. While he was there, a wealthy textile merchant, George Fabyan, who maintained laboratories in acoustics, chemistry, genetics, and cryptology (to try to prove that Bacon wrote Shakespeare's plays) on his 500-acre estate, Riverbank, at Geneva, Illinois, decided that he needed a geneticist to improve the grains and livestock on his farm. He applied to Cornell for a "would-be-er," not an "as-is-er," and hired Friedman, to begin June 1, 1915.

Fabyan was a man of no formal education but of intelligence and energy. He had a great desire to be "somebody," and that desire motivated his subsidizing the Baconian studies: proof of this revolutionary thesis would cover its patron as well as its actual discoverers with glory. He himself read little, but he absorbed enough from those around him to make his talk on almost any subject sound impressive—at least superficially. He was autocratic, never allowing his staff to disagree with him, but otherwise not unpleasant so long as employees recognized that he was boss. A cardinal article of faith with him was that a well-executed sales campaign could put across almost anything.

Friedman did some genetics work for him, but, because he was handy with a camera, he helped the cryptologists who were looking for Bacon's cipher signatures in Shakespeare by making photographic enlargements of the Elizabethan printing that figured in the work. The Department of Ciphers of the Riverbank Laboratories consisted of 14 or 15 high-school and college graduates who assigned the individual letters in these Elizabethan texts to one or the other of two fonts of type as part of the Baconian search. Fabyan gave them their living plus a salary of about $50 a month. The staff was fed and housed in Engledew and Hoover Cottages, the cipher laboratories taking up the first floor of Engledew.

The young woman who collated the work of many of the other staff members was Elizebeth Smith. She had been , born August 26, 1892, in Huntington, Indiana, the youngest of the nine children of John M. Smith, a dairyman, banker, and county Republican committeeman, and his wife, Sopha, who spelled her daughter's Christian name witb an *e* instead of an a in the middle because she was not going to have anyone calling her child "Eliza." After completing high school in Huntington, Elizebeth attended Wooster College briefly but was graduated from Hillsdale College in Michigan where she had majored in English. While working at the Newberry Library in Chicago, she was recruited by Fabyan and began work there in 1916.

Neither she nor Friedman had given any particular previous thought to cryptology, but they began to get personally interested in the work. It is yet another of the ironies of cryptologic history that the interest of two foremost cryptologists was aroused by a false doctrine—a doctrine, moreover, against which they later were to wage a lifetime battle. For at table at the Riverbank cottages they heard gaudy tales of lusty Elizabethan life, of the not-so-Virgin Queen, of courtiers' intrigues and the secret histories of the great names of English history—all actually invalid decipherments of Shakespeare's plays tending to prove that Bacon had written them, related by the gentle, upright, but self-deluded woman who had "deciphered" them, Mrs. Elizabeth Wells Gallup. These stories stirred Friedman's dormant interest; he began to do some of the cryptology, and inevitably its puissant magic seeped like the fume of poppies into his mind and spirit and intoxi-

caiea mm. "When it came to the cryptology," he recalled years later, "something in me found an outlet."

An understatement. He soon found himself head of the Department of Ciphers as well as the Department of Genetics at Riverbank. The attraction he felt for cryptology was reinforced by the attraction he felt for a cryptologist: the quick-witted and sprightly Miss Smith. In May of 1917 they were married and started the most famous husband-and-wife team in the history of cryptology.

America had declared war a month before, and River-bank, which had the only going cryptologic concern in the country, began getting, on an informal basis, cryptograms for solution from various government bureaus. Probably the most important were messages to and from a ring of 125 Hindus who, with German aid, were taking advantage of England's preoccupation in Europe to strike for Indian independence. The intercepts were given to Friedman for solution, and he quickly solved the number cipher used in cablegrams to Berlin. The letters of the plaintext and of the keyword were transformed into digits by means of a 4 X 7 checkerboard with a normal alphabet; the key digits were then added to those of the plaintext to form the ciphertext. One key was LAMP. Each agent had his own key, but Friedman had no trouble in solving them. Nor was he stumped by a system usually regarded by amateurs as the ne plus ultra of cryptographic security: a book cipher.

It came to him in the form of a seven-page typewritten letter. The writer, Heramba Lai Gupta, had enciphered only the important words, leaving large patches of clear-text as valuable clues; he had also repeated the equivalents for many letters instead of seeking new ones and had employed neighboring letters in a single line, thus enabling Friedman to reconstruct the words of the keytext as a check upon and aid to the solution. For example, Friedman guessed from context that 83-1-2 83-1-11 83-1-25 83-1-1 83-1-8 83-1-13 83-1-18 83-1-3 83-1-1 83-1-6 83-1-3 83-1-6 meant *revolution in,* with the 83 the page, the 1 the line on that page, and the third number the letter in that line. (It is interesting to note how the third group sticks out as the equivalent for a low-frequency letter by being so far back in the line.) This gave him OKI . . N . L . . E . *u* . . as the start of the key line, and this in turn probably let him guess that the line started with *original* or *originally.*

[Codebreakers 187.jpg]

*How the Hindus worked the book cipher that William Friedman solved*

He would then have known that 83-1-4 in the very next word was the equivalent for *g* in *Bengal*. By taking full advantage of such clues he built up the entire plaintext without ever knowing what was later

discovered—that the key book was Price Collier's *Germany and the Germans,* a scholarly work published in New York in 1913.

The Hindus were prosecuted for trying to purchase the uprising's arms in the United States and to ship them from the West Coast. At the mass trials in Chicago and San Francisco, Friedman gave evidence that in effect convicted the conspirators out of their own mouths. The San Francisco proceeding witnessed one of the most dramatic scenes ever to occur in an American courtroom when one defendant rose, fired two shots from a revolver to assassinate a compatriot who was testifying for the government, and was himself killed by a marshal shooting over the heads of the crowd. In an anticlimax, a jury later found most of the defendants guilty.

A few months after these Hindu solutions, the British submitted five short messages to Riverbank for tests. They had been enciphered by a cipher device invented by J. St. Vincent Pletts of M.I. l(b), the British War Office cryptanalytic bureau. The machine, to serve in the field, shifted its cipher alphabet irregularly by means of gears. So highly did the British regard it that one argument advanced against its adoption was that if the Germans captured one and adopted it, the Allies would no longer be able to solve enemy messages! Friedman, however, at once recovered the keyword CIPHER to one of the mixed alphabets. But he could not seem to get anywhere with the other keyword and, stymied, he resorted to a bit of psychological cryptanalysis. He turned to the new Mrs. Friedman, and asked her to make her mind a blank.

"Now," he went on, "I want you to tell me the first word that comes into your mind when I say a word." He paused. "Cipher," he said.

"Machine," she replied.

It turned out to be the very key desired. Three hours after Friedman received the cryptograms, their plaintexts were being cabled to London. (The first one read, in a phrase dear to proud inventors, *This cipher is absolutely undecipherable.)* Needless to say, it ended consideration of the Pletts device for Allied use.

In addition to this cryptanalytical work, Friedman did most of the teaching of a class of Army officers sent in the fall of 1917 to Riverbank's Department of Ciphers to learn cryptology. For instruction in these courses, he

turned out a series of technical monographs. He completed seven before he went overseas to o.2 A.6 in the spring of 1918 and wrote an eighth on his return. Known collectively as the Riverbank Publications, they rise up like a landmark in the history of cryptology. Nearly all of them broke new ground, and mastery of the information they first set forth is still regarded as the prerequisite for a higher cryptologic education.

Riverbank Publication No. 22, written in 1920 when Friedman was 28, must be regarded as the most important single publication in cryptology. It took the science into a new world. Entitled *The Index of Coincidence and Its Applications in Cryptography,* it described the solution of two complicated cipher systems. Friedman, however, was less interested in proving their vulnerability than he was in using them as a vehicle for new methods of cryptanalysis.

In it, Friedman devised two new techniques. One was brilliant. It permitted him to reconstruct a primary cipher alphabet without having to guess at a single plaintext letter. But the other was profound. For the first time in cryptology, Friedman treated a frequency distribution as an entity, as a curve whose several points were causally related, not as just a collection of individual letters that happen to stand in a certain order for noncausal (historical) reasons, and to this curve he applied statistical concepts. The results can only be described as Promethean, for Friedman's stroke of genius inspired the numerous, varied, and vital statistical tools that are indispensable to the cryptology of today.

Before Friedman, cryptology eked out an existence as a study unto itself, as an isolated phenomenon, neither borrowing from nor contributing to other bodies of knowledge. Frequency counts, linguistic characteristics, Kasiski examinations—all were peculiar and particular to cryptology. It dwelt a recluse in the world of science. Friedman led cryptology out of this lonely wilderness and into the broad rich domain of statistics. He connected cryptology to mathematics. The sense of expanding horizons must have resembled that felt by chemists when Friedrich Wohler synthesized urea, demonstrating that life processes operate under well-known chemical laws and are therefore subject to experimentation and control, and leading to today's vast strides in biochemistry. When Friedman subsumed

cryptanalysis under statistics, he likewise flung wide the door to an armamentarium to which cryptology had never before had access. Its weapons—measures of central tendency and dispersion, of fit and skewness, of probability and sampling and significance—were ideally fashioned to deal with the statistical behavior of letters and words. Cryptanalysts, seizing them with alacrity, have wielded them with notable success ever since.

This is why Friedman has said, in looking back over his career, that *The Index of Coincidence* was his greatest single creation. It alone would have won him his reputation. But in fact it was only the beginning.

He and Mrs. Friedman quit Riverbank near the end of 1920. The situation had become intolerable. Fabyan had lured him back after the war with raises and promises of absolute freedom to prove or disprove the existence of ciphers in Shakespeare. But he had squelched every attempt to do so and had embarrassed Friedman into apparently acquiescent silence at lantern-slide lectures on the subject. On January 1, 1921, Friedman began a six-month contract with the Signal Corps to devise cryptosystems. When it expired, he was taken on the civil-service payroll of the War Department at $4,500 a year.

One of his first assignments was to teach a course in military codes and ciphers at the Signal School, then at Camp Alfred Vail, New Jersey. For this he wrote a textbook that, for the first time, imposed order upon the chaos of cipher systems and their terminology. These had sprouted in a bewildering variety, and writers treated each as individual and special cases. Friedman sorted them out on the basis of structure instead of aspect, and so logical and useful was this classification that it has become standard. He modeled his nomenclature on his categories, so that the names he minted have the great merit of making the relations between the various genera of ciphers evident on sight. An example is the complementary pair "mono-alphabet" and "polyalphabet"; the French were still calling polyalphabetic systems by the almost obfuscatory "double substitution," which tells absolutely nothing at all about the system. Friedman's most important coinage was the word "cryptanalysis," which he devised in 1920 to clear up a chronic source of confusion in cryptology—the ambiguity of the verb "decipher," then used to mean both

authorized and unauthorized reductions of a cryptogram to plaintext. He titled his book *Elements of Cryptanalysis,* and the term has so prospered that today it circulates in general conversation and print.

While the book's main contribution is its taxonomy, each of its 143 pages of text manifests the author's concern for always making clear to the reader why things happen as they do. As a result, the student understands principles and phenomena, and the lessons stick. Partly because of this pedagogical effectiveness, partly because of its substantive values, Friedman's book, issued by the Chief Signal Officer in May of 1923 as Training Pamphlet No. 3, has guided the development of all American cryptology since then.

At the start of 1922, Friedman became Chief Crypt-analyst of the Signal Corps in charge of the Code and Cipher Compilation Section, Research and Development Division, Office of the Chief Signal Officer. To help him carry on the work of the office he had a single clerk-typist—a cauliflower-eared ex-prizefighter. Because Yard-ley's Black Chamber was doing the cryptanalysis for the War Department, Friedman's functions were nominally cryptographic. He installed the M-94—the Jefferson wheel cipher—as the Army's field cipher. Paradoxically, however, his job involved a great deal of cryptanalysis. He was continually testing the new systems of cryptography urged on the Army as "absolutely indecipherable" by zealous amateurs.

Most difficult of these was the machine with five wired codewheels—rotors—invented by Edward H. Hebern, whose principle became the most widely used in high-level cryptography during World War **II.** The device produces a cipher of hideous nightmare complexity. Friedman sorted it out and reconstructed the wiring of the rotors. This work was of the utmost importance, for it laid the foundations for the PURPLE machine solution and for today's many solutions of modem rotor machines. The technique was far in advance of its time. So far as is known, not another cryptanalyst on the globe could duplicate it—and none did, apparently, for more than two decades. With this solution of Friedman's, world leadership in cryptology passed to America.

Meanwhile, the Army had been studying its divided cryptologic operation and, shortly before tie State Depart-

ment withdrew support from Yardley's bureau, hac decided to integrate both cryptographic and cryptanaJytic functions in the Signal Corps. The closing of the Black Chamber eased the transition, and on May 10, 1929, cryptologic responsibility devolved upon the Chief Signal Officer. To better meet these new responsibilities, the Signal Corps established a Signal Intelligence Service in its War Plans and Training Division, with Friedman as director. Its officially stated mission was to prepare the Army's codes and ciphers, to intercept and solve enemy communications in war, and in peace to do the training and research —a vague enough term—necessary to become immediately operational at the outbreak of war. To carry out these duties, Friedman hired three junior cryptanalysts, all in their early twenties, at $2,000 a year—the first of the second generation of American cryptologists. They were Frank Rowlett, a Virginian, and Solomon Kullback "and Abraham Sinkov, close college friends who had taught together in New York City high schools before coming to Washington and who both received their Ph.D.'s in mathematics a few years later. It was the beginning of an expanion that led to the PURPLE solution, the triumphs of World War II, and the massive cryptologic organization of today. At his death on November 2, 1969, he was widely regarded as the greatest cryptologist that science had ever seen.

By this time the Navy, too, had its cryptologic section. Like the Army's, it had evolved gradually.

Naval participation in the 1917 war was too limited for cryptanalytic development, but interest was stimulated. Accordingly, in January of 1924, Lieutenant Laurance F. Safford was ordered to set up a radio intelligence organization in the Code and Signal Section. When he left for sea duty two years later, a small, highly secret organization was functioning in Room 2646 of the "temporary" Navy Department building on Constitution Avenue. Lieutenant Ellis M. Zacharias, who trained seven months in 1926 with the cryptanalytic organization, told what it was like:

> My days were spent in study and work among people with whom security had become second nature. Hours went by without any of us saying a word, just sitting in front of piles of indexed sheets on which a mumbo jumbo of figures or letters was displayed in chaotic

disorder, trying to solve the puzzle bit by bit like fitting together the pieces of a jigsaw puzzle. We were just a few then in Room 2646, young people who gave ourselves to cryptography with the same ascetic j;' devotion with which young men enter a monastery. It ';•: was known to everyone that the secrecy of our work '! would prevent the ordinary recognition accorded to other accomplishments. It was then that I first learned that intelligence work, like virtue, is its own reward.

On completion of his apprenticeship, Zacharias took charge of an intercept post on the fourth floor of the American consulate in Shanghai to learn as much as he could from Japanese naval messages. Safford returned to cryptology in June, 1929, and, except for a four-year tour at sea from 1932 to 1936, stayed with the science from then on. He built up the communications intelligence organization into what later became OP-20-G and, by adding improvements of his own to Edward Hebern's rotor mechanisms, gradually developed cipher machines suitable for the Navy's requirements of speed, reliability, and security. His contributions to cryptanalytics were minor, since his talents lay more in the administrative and mechanical fields. But he is the father of the Navy's present cryptologic organization.

## 11. Secrecy for Sale

ON A MORNING in December of 1917, a rather handsome young man of 27 hurried through the colonaded lobby of the American Telephone & Telegraph Company at 195 Broadway in downtown Manhattan. He rode the elevator up to the 17th floor, where he worked in the telegraph section of the company's development and research department. This section, composed of some of the brightest engineers in the company, was concentrating on the newest development in telegraphy, the printing telegraph or teletypewriter.

Gilbert S. Vernam was—if things were as usual—a little late that morning. He nearly always was, and, his

boss said, "It used to burn me up to see him come sneaking in and slink into his seat." The yearbook of his alma mater, Worcester Polytechnic Institute, had wondered "what would happen to Tech if 'Tau' should accidently get to class on time in the morning."

A native of Brooklyn, Vernam was graduated from the Massachusetts college, where he had been president of the Wkeless Association and had been elected to Tau Beta Pi, the engineering honorary society, in 1914, after having spent a year working. He immediately joined A. T. & T. and, a year later, married a Brooklyn girl, Alline L. Eno. They had one child. Vernam was a clever young man— one of the stories about him has him stretched on his couch each evening wondering aloud, "What can I invent now?" He had the rare type of mind that can visualize an electrical circuit and put it down on paper without having to try it out with wires. He did so well in the telegraph section that its head, Ralzemond D. Parker, assigned him to a special secrecy project. And late though he may have been that winter morning, Vernam had brought a bright idea to work with him. Quiet and unassuming, though with a droll sense of humor, he probably put forth his suggestion with diffidence, but his co-workers on the secrecy project saw at once that he had something.

The project had begun during the summer, a few months after war had been declared, when Parker directed some of the telegraph section members to investigate the security of the printing telegraph. Would its very newness, the fact that the enemy might not have developed such means, guard its messages? The secrecy group soon found that it did not. The fluctuations of the current could be recorded by an oscillograph and the messages read with ease. Even multiplexing—sending several messages simultaneously in both directions over a single wire—offered no real security. The engineers resolved the oscillograph undulation into its constituent curves and read the eight individual messages. The group discussed altering connections inside the printing telegraph mechanism. This would have the effect of enciphering one letter into another in a monoalphabetic substitution. The engineers realized that this offered no real secrecy but, stymied, did not pursue the matter until Vernam bounded in with his idea.

It was based upon the Baudot code, the Morse code of

the teletypewriter. In this code, named for its French inventor, J.M.E. Baudot, each character is allotted five units, or pulses. Each unit consists of either an electrical current or its absence in a given time. There are, consequently, 32 different combinations of marks and spaces, and a combination is assigned to each character—26 for the letters and one each for the six "stunts" (space between words, shift up to numbers and punctuation marks, shift back down to letters, return type-carriage to left side of paper, feed paper up a line, and idle). Through an electrical arrangement involving rotating commutators, the proper sequence of pulses is sent out when a character's key is struck on the keyboard. For example, *a* is *mark mark space space space, i* is *space mark mark space space* and the figure shift is *mark mark space mark mark.* At the receiving end, the incoming pulses energize electromagnets that, in combination, select the proper character and print it. In the punched paper tape which is frequently used to run teletypewriters, marks are represented by holes and spaces by leaving the tape intact. To read the tape, metal fingers push through the holes to make contact and thereby send pulses; where there is a space, the paper keeps the fingers from completing the circuit.

Vernam suggested punching a tape of key characters and electromechanically adding its pulses to those of the plaintext characters, the "sum" to constitute the ciphertext. The addition would have to be reversible so that the receiver could subtract the key pulses from the cipher pulses and get the plaintext. Vernam decided upon this rule: If the key and the plaintext pulses are both marks or both spaces, the ciphertext pulse will be a space. If the key pulse is a space, and the plaintext a mark, or vice versa—if, in other words, the two are different—the ciphertext pulse will be a mark. The four possibilities are these:

| *plaintext* | | *key* | | *ciphertext* |
|---|---|---|---|---|
| mark | + | mark | = | space |
| mark | + | space | = | mark |
| space | + | mark | = | mark |
| space | + | space | = | space |

Decipherment is unambiguous. For example, with cipher-text *mark* and key *space* only *mark* is possible for the

plaintext. The whole system may be set out in a single, compact table. Using the convenient notation of 1 for *mark* and 0 for *space,* the rule would be tabulated as follows:

*plaintext* 1 0

*key*

*0*

*0 1*

*1 0*

*ciphertext*

In accordance with this rule, Vernam combined the five pulses of the plaintext character with the five of the key character to obtain the five pulses of the ciphertext character. Thus, if the plaintext is *a,* or 11000, and the key is 10011, which happens to be B, the encipherment is this:

*plaintext key*

*ciphertext*

11000 10011

0101 1

At the receiving end, the key pulses are applied one by one to the successive ciphertext pulses; the rule determines the plaintext pulses. With cipher pulses 10100, and the key pulses 00110, the plaintext would be:

*ciphertext* 10100

*key* 00110

*plaintext* 1 0 0 1 0, or *d.*

To combine the pulses electrically Vernam devised an arrangement of magnets, relays, and bus-bars. Since encipherment and decipherment were reciprocal, the same arrangement served for both. He fed the pulses into this device from two tape readers—one for a keytape, the other for the plaintext tape. The mechanism closed a circuit, resulting in a mark, when the two incoming pulses were different, and opened a circuit, resulting in a space, when they were the same. This output of marks and spaces could be transmitted just like an ordinary teletypewriter message to the receiver. Here the Vernam apparatus sub-

tracted out the key pulses, which were supplied by an identical keytape, and recreated the original plaintext pulses. These it would channel into a teletypewriter receiver, which would print out the plaintext, just like a news ticker in a city room.

That was the beauty of it. No longer did men have to encipher or decipher a message in a separate step (though they still had to prepare keytapes, insert them in the apparatus, etc., since doing away with these would dispense with secrecy altogether). Plaintext went in and plaintext came out, while anyone intercepting the message between the two endpoints would pick up nothing but a meaningless sequence of marks and spaces. Messages were enciphered, transmitted, received, and deciphered in a single operation—exactly as fast as a message in plain English. The advantage was not the mechanical enciphering and printing of the message. That had been accomplished as far back as the early 1870s by two Frenchmen, fimile Vinay and Joseph Gaussin—though not with the speed and ease of a typewriter keyboard. Rather it was the assimilation of encipherment into the overall communication process. Vernam created what came to be called "on-line encipherment" (because it was done directly on the open telegraph circuit) to distinguish it from the old, separate, off-line encipherment. He freed a fundamental process in cryptography from the shackles of time and error. He eliminated a human being—the cipher clerk—from the chain of communication. His great contribution was to bring to cryptography the automation that had benefited mankind so much in so many fields of endeavor.

These values were immediately recognized, and Ver-nam's idea quickly kicked up a flurry of activity. He put it down on paper in a sketch dated December 17. A.T. & T. notified the Navy, with which it had worked closely in a communications demonstration the previous year, and on February 18, 1918, Vernam, Parker, Lyman F. Morehouse, equipment engineer of the telephone company, and Edward Watson explained the Vernam system, together with some other possibilities, to a Lieutenant Griffiths. On March 27, the engineers conferred with colleagues of the Western Electric Company, A. T. & T.'s manufacturing subsidiary, and began constructing a couple of Vernam devices, using as many standard parts as

I

possible. They hooked them up to two teletypewriters and,-in the Western Electric laboratory, ran the first tests of what the engineers called "automatic cryptography." The devices worked like a charm. A. T. & T. reported this to the Army. Major Joseph O. Mauborgne, then head of the Signal Corp's research and engineering division, came, saw and was conquered. Except for the problem of the keys.

In the first days of development, the Vernam keys took the form of loops of tape perforated with characters drawn from a hat, giving a random keytext. The engineers, who were rapidly learning about cryptology, probably from a 1916 manual, soon spotted the flaw in this. The Vernam system is a polyalphabetic. A 32 X 32 tableau may be set up with the 32 characters of the Baudot alphabet across the top as plaintext and down the side as keys. Because the Baudot alphabet is public information, the composition of the 32 cipher alphabets filling the body of the tableau would be known. Secrecy in the Vernam system thus resides entirely in its keys. Looped keytapes would pass through the Vernam mechanism at regular intervals, permitting a simple Kasiski solution, even though the key recovered would be incoherent. The engineers made the keytapes extremely long to increase the difficulty of such a solution. But then the keytapes became too hard to handle.

Engineer Morehouse surmounted these difficulties by combining two short keytapes of different lengths in a Vernam device as if one were enciphering the other and using the extremely lengthy output—called the secondary key—as the key for plaintext. If one loop were 1,000 characters long and the other 999, the one-character difference would produce 999,000 combinations before the sequence would repeat. Thus two tapes each about eight feet long would breed a key that would extend 8,000 feet on a single tape. This was a major practical improvement.

But Mauborgne recognized that even this system was not immune to cryptanalysis. The future Chief Signal Officer, then 36, was an extraordinary cryptanalyst. He had studied the subject at the Army Signal School with an expert, was thoroughly conversant with its techniques, had devised a solution for the hitherto unsolved Playfair, and almost certainly knew of Friedman's Riverbank Publications, including No. 17 on solving running-key cryptograms. He therefore saw that heavy traffic raised the possibility of a Kerckhoffs superimposition, even with the

two-tape system. Moreover, probable words would enable the cryptanalyst to recover the secondary key. He could then test the various possibilities for the two primary keys at intervals of 999 and 1,000 letters, and so gradually build them up. Mauborgne demonstrated this to the A. T. & T. engineers with the keywords RIFLE and THOMAS.

Mauborgne had himself perhaps participated in work at the Army Signal School several years earlier that had concluded (before Friedman's solution) that the only safe running key was, in Parker Hitt's words, one "comparable in length with the message itself." Mauborgne's study of the A. T. & T. system brought this home to him more forcefully. Any repetition of any kind in the keys of cryptograms under analysis imperils them and perhaps dooms them to solution. It does not matter whether the repetitions lie within a single message or among several, arise from the interaction of repeating primary keys or from the simple repeating of a single long key. Repetitions in the key could not be permitted. At the same time, Friedman's work had demonstrated that running keys could not be intelligible. To avoid the Scylla of repetition and the Charybdis of intelligibility, keys would have to be, Mauborgne realized, both endless and senseless. He therefore welded together the randomness of the key, created, perhaps almost accidentally, by Vernam, and the non-repetition of the key, discovered by the Army Signal School cryptologists, into what is now called the "one-time system." It consists of a random key used once, and only once. It provides a new and unpredictable key character for each plaintext character in the whole ensemble of messages ever to be sent by a group of correspondents.

And it is an unbreakable system. Some systems are unbreakable in practice only, because the cryptanalyst can conceive of ways of solving them if he had enough text and enough time. The one-time system is unbreakable both in theory and in practice. No matter how much text a cryptanalyst had available in it, or how much time he had to work on it, he could never solve it. This is why:

To solve a polyalphabetic cipher is essentially to gather all the letters that are enciphered in a single alphabet into a homogeneous group that may be studied for its linguistic traits. The techniques of this collection differ, as do the kinds of keys. Thus a Kasiski examination sifts out the

identically keyed letters in a repeating key. A running key with a coherent text can be solved by reciprocally reconstructing the plaintext and the keytext. A running key with a random text used in two or more messages succumbs to a simultaneous reconstruction of the two plaintexts, one checking the other. Other polyalphabetics, such as the autokey and the two-tape system, engender specialized solutions that stem from their own peculiarities. The monoalphabetically enciphered letters that are the goal of these techniques also exist in a Vernam one-time system cryptogram because the 32 available cipher alphabets are used over and over again. But the cryptanalyst has no way of sorting them out because the key in a one-time system neither repeats, nor recurs, nor makes sense, nor erects internal frameworks. Hence, his methods, all based in one way or another on these characteristics, all fail. The perfect randomness of the one-time system nullifies any horizontal, or lengthwise, cohesion, as in coherent running key or autokey, and its one-time nature bars any vertical assembly in Kasiski or Kerckhoffs columns, as in keys repeated in a single message or among several messages. The cryptanalyst is blocked.

How about trial and error? It seems as if brute testing of all possible keys, one after another, would eventually yield the plaintext. Success this way is an illusion. For while exhaustive trials would indeed bring out the true plaintext, they would also bring out every other possible text of the same length, and there would be no way to tell which was the right one. Suppose that the cryptanalyst deciphers a four-letter military message with every key, beginning with AAAA. He strikes plaintext at key AABI: *kiss.* Unlikely in this context. He presses on. Key AAEL yields plaintext *kill.* Better—but he wants to make sure. He continues through key AAEM, giving *kilt,* which might be an oblique reference to a Scottish maneuver, and AAER, *kiln.* Further down the line he reaches *fast* at GZBM and *slow* at KHIA, *stop* at HRIW and *gogo* at XSTT, *hard* at PZVQ and *easy* at RZBU. He finds when he ends at ZZZZ that he has merely compiled a list of every possible four-letter word—the hard way. He can no more pick the right solution from this list than he can from a dictionary of military terms. The key does not help in limiting the selection because, since it is random, any group of four letters is as acceptable a keytext as

any other. The worst of it is that the possible solutions increase as the message lengthens. There are only three possible solutions for a one-letter cryptogram, but dozens for those of two letters, and zillions for those of 100.

A final hope flickers. Suppose that the cryptanalyst obtains the plaintext of a given cryptogram, perhaps through theft or the error of a radio operator. Can he use the key that he can recover to determine the system on which that key was built, and so predict future keys? No, because a random key has no underlying system—if it did, it would not be random.

These are empiric proofs. It is possible, however, to demonstrate a priori that the one-time system is unbreakable. This constitutes the proof that it is theoretically unbreakable.

In essence, the Vernam encipherment constitutes an addition—an addition based on the Baudot alphabet, but an addition nonetheless. Suppose then that the plaintext is 4 and the key is 5. The ciphertext will be 9. Now, given only this, the cryptanalyst has no way of knowing whether it results from the addition of 7+ 2, or 6+ 3, or — 2 + 11, or 4 + 5, or any other of the 32 possible combinations. Generalized, the situation is $x + y = 9$. Mathematicians call this an equation in two unknowns, and a single such equation has no unique solution. Two equations with the same two unknowns are required. The one-time system prevents the cryptanalyst from ever bringing two or more such equations together. The utter absence of any pattern whatsoever within its key precludes him from finding two occurrences of a given key character by reconstructing a pattern. And the tape's exhaustless novelty makes it impossible for him to locate these occurrences in any key repetitions. The cryptanalyst is thus denied any chance of getting additional information to delimit one of the unknowns; he is left with all 32 possibilities for the key character, and consequently all 32 for the plaintext. True it is that in the cryptanalytic case of an equation in two unknowns, some solutions are more probable than others. Thus, there is a 12 per cent chance that the plaintext unknown is *e,* an 8 per cent chance that it is *t,* and so on down the frequency table. But this does not answer the cryptanalyst's question, for it does not specify which of these probabilities is actually present in the individual case before him.

So the answers again evade the cryptanalyst. Formless, endless, the random one-time tape vanquishes him by dissolving in chaos on the one hand and infinity on the other. Here indeed the cryptanalyst gropes through caverns measureless to man. His quest is Faustian; who would dare it would know more than can be known.

Why, then, is this ultimate cipher not in universal use? Because of the stupendous quantities of keys required. The problems of producing, registering, distributing, and canceling the keys may seem slight to an individual who has not had experience with military communications, but in wartime the volumes of traffic stagger even the signal staffs. Hundreds of thousands of words may be enciphered in a day; simply to generate the millions of key characters required would be enormously expensive and time-consuming. Since each message must have its unique key, application of the ideal system would require shipping out on tape at the very least the equivalent of the total communications volume of a war. In fact, however, considerable extra key material would have to be supplied. A group of subordinate units may possess some tape in common for intercommunication, but once one unit uses a roll of keytape, the others must cancel their identical rolls. In practice, this step is the most difficult. It is virtually impossible in the hubbub of battle to monitor the messages of a dozen other units to determine what keytapes they have used.

In general, the physical problems bar employing a onetime system in a fluid situation, such as military operations in the field. These difficulties do not hold for more stable situations, such as exist at high military headquarters, at diplomatic posts, or in a two-way spy correspondence— and in such situations one-time systems are practicable and are used. Even here, however, difficulties arise if traffic volume is heavy.

But though the device was an engineering success, it proved a commercial failure. Cable companies and business firms, which A. T. & T. hoped would buy cipher attachments for its teletypewriters, passed it over in favor qf the old-fashioned commercial codes, which substantially shortened messages, thereby cutting cable tolls, and which gave a modicum of secrecy as well. The armed forces budgets had shrunk to their peacetime tightness; crypto-logically, the physical difficulties forced Army communi-

cators back onto the two-tape system, and the demonstrated solvability of this threw the whole Vernam arrangement into temporary limbo.

The Army revived it in a hurry as SIGTOT when World War II loomed, but by then Vernam was well out of it. He had continued developmental work at A. T. & T. for several years. He improved his own system,* invented a device for enciphering handwriting during telautograph transmission, and came up with one of the earliest forms of binary digital encipherment of pictures—another precocious development. He was so good that he was grabbed off at a substantial raise by International Telephone and Telegraph Corporation's research subsidiary, International Communication Laboratories, which was doing some cryptographic work. Four months later the stock market crashed. Vernam, with no seniority, was soon out. He went to Postal Telegraph Cable Company, which merged with Western Union. His inventive spark flared from time to time, and he was granted 65 patents in all, among them such important noncryptologic items as the semiautomatic torn-tape relay system, the push-button switching systems, and finally the fully automatic telegraph switching system, all for the Air Force's 200,000-mile domestic network.

But the reversal in his personal fortunes seemed to depress him. Each night he sank deeper and deeper into the newspaper. Finally, on February 7, 1960, after a long bout with Parkinson's disease, the man who had automated cryptography died in obscurity in his home in Hackensack, New Jersey.

The history of science is replete with coincidence. Adams and Leverrier deduced the existence of Neptune almost simultaneously. While Darwin was elaborating his theory of evolution, Wallace sent -him a short paper that succinctly set it forth. Five years after Morse invented his telegraph, Wheatstone independently invented another. So it is not surprising that coincidence brushed cryptography

*In its original form, the ciphertext included the stunt characters. This made it difficult to record the ciphertext on paper. The sudden appearance of a figure shift would abruptly convert a literal cryptogram into one of numbers and punctuation marks. A carriage return without a paper feed would result in an overline. To prevent this, Vernam added some circuits that would cause the stunts to print as two-letter groups.

in the crucible years of the First World War and just after. Its fabled long arm reached out and tapped four men in four countries. Spurred by the vast wartime use of secret communications, and beckoned by the new age of mechanization, they independently created the machine whose principle is perhaps the most widely used in cryptography today. This principle is that of the wired code-wheel, the rotor.

The body of a rotor consists of a thick disk of insulating material, such as Bakelite or hard rubber, commonly two to four inches in diameter and half an inch thick. Embedded around the circumference of each face are 26 evenly spaced electrical contacts, often of brass. Each contact is connected at random by a wire to a contact on the opposite face. Thus a path for an electric current is set up that starts at one point on the circumference of one side and ends at another point on the other.

The contacts on the starting, or input, face represent plaintext letters and those on the output face ciphertext letters. The wire connections between the two then provide a way of converting plaintext letters to ciphertext. To encipher, one need only fire a burst of current into the rotor at the input contact of the desired plaintext letter, say, *a;* this current then courses along the wire to emerge at an output contact representing the ciphertext letter, say, R. If a list be drawn up of all the rotor's wire connections from the plaintext to the ciphertext face, it will constitute a monalphabetic substitution alphabet. The rotor thus embodies a cipher alphabet in a form suitable for electro-mechanical manipulation.

When the rotor turns, however, the current entering at a specific point will no longer emerge at the same point as before. The plaintext letter that in the previous position was enciphered to x is now enciphered to something entirely different. The rotor thus will produce as many cipher alphabets as it has positions, usually 26. Now, several rotors may be placed side by side. The current that represents a letter will traverse their internal maze to encipher that letter. A turn of any rotor will alter that maze and so change the letter's encipherment. If each rotor turns a space only when the preceding rotor has completed a revolution, the number of alphabets that the array of rotors creates will equal the product of the number of positions that each rotor can take. Five rotors,

each with 26 positions, will thus generate 11,881,376 cipher alphabets. This hemmorhaging profusion will provide a different alphabet for each letter in a plaintext longer by far than the complete works of Shakespeare, *War and Peace,* the *Iliad,* the *Odyssey, Don Quixote,* the *Canterbury Tales,* and *Paradise Lost* all put together.

A period of that length thwarts any practical possibility of a straightforward solution on the basis of letter frequency. This general solution would need about 50 letters per cipher alphabet, meaning that all five rotors would have to go through their combined cycle 50 times. The cryptogram would have to be as long as all the speeches made on the floor of the Senate and the House of Representatives in three successive sessions of Congress. No cryptanalyst is likely to bag that kind of trophy in his lifetime; even diplomats, who can be as verbose as politicians, rarely scale those heights of loquacity.

Consequently the cryptanalyst must fall back on special cases. They furnish him with what he must have for a practicable rotor solution: the plaintext for a length of ciphertext. He can get this in several ways. A Kerckhoffs superimposition is possible when several messages begin at the same rotor setting, or with settings so close to one another that the cipher-alphabet sequence overlaps among messages. Statistical tests will reveal these. Sometimes two cryptograms have the same plaintext: one was sent in the wrong key, or identical orders are being sent to several units. Probable words or stereotyped beginnings will sometimes provide good clues. And sometimes the plaintext itself becomes available, through wireless queries, a cipher clerk's carelessness, published diplomatic notes, and the like. All of these situations have occurred often enough for the cryptanalyst to exploit them.

That exploitation entails resolving the millions of secondary alphabets into the few primary ones. It calls upon the resources of higher mathematics, especially group theory, whose techniques are particularly suited to handle the many unknowns involved in a rotor solution. Basically these unknowns are the paths taken by the wires of each rotor from one face to the other. The cryptanalyst-mathe-matician quantifies them by measuring the distance, or displacement, between the input and the output contacts. For example, a wire from input contact 3 to output contact 10 marks a displacement of 7. Similarly, letters are given

numerical values, usually a = 0, 6 = l,...z = 25. Using his known or assumed plaintext values, the cryptanalyst sets up equations in which the displacements of the several rotors constitute the unknowns, and then, using higher algebra, solves the equations for them. By repeating this process, the cryptanalyst can list the differences between many of the displacements on the rotor. He can then seek an arrangement of wires having these differences that will reproduce the known cryptographic effects. In similar fashion, he will reconstruct another rotor. Such are the basic principles of the rotor solution. But their practice wracks the cryptanalyst with some of the most excruciating mental torture known to man. And so the rotor system produces an extremely complex and secure cipher from simple elements in a simple construction. Who are the four contrivers of this miniature labyrinth, the four modern Daedaluses of cryptography?

The inventor of the first machine to embody the rotor principle gave the best efforts of his life to it. Edward Hugh Hebern was born April 23, 1869, in Streator, Illinois, and was raised in the Soldiers' Orphan Home in Bloomington. When he was 14 he began living and working on a farm near Odin, where he got a high school education. He headed West at 19, and, after selling a timber claim in California to a sawmill where he worked for a time, he turned to carpentry and built and sold houses in Fresno. Soon after he turned 40, he somehow became interested in cryptology. Hebern was at this time a blue-eyed, brown-haired man of medium height and build, mustachioed, quiet, a great reader, kind, and even-tempered.

From 1912 to 1915, he filed for patents for cryptographic check-writing devices, cipher keyboards for typewriters, movable letter blocks to form mixed reciprocal monoalphabets, and a ciphering typewriter. In 1915, he devised an arrangement in which two electric typewriters were connected by 26 wires in random fashion; thus when a letter was struck on the plaintext keyboard, it would cause a ciphertext letter to print on the other machine. Since the wires remained plugged into the same jacks during an entire message, the cryptogram would be monoalphabetic—but it would have been electromechan-ically enciphered.

The wire interconnections comprised the germ of the rotor—a means to vary the monoalphabetic encipherment. In 1917, Hebern reduced his ideas to the first drawings made of a rotor system, which, a year later, grew into actual apparatus.

Early in 1921, he advertised an "unbreakable" cipher in a marine magazine, but Miss Agnes Meyer, a crypt-analyst in the Navy's Code and Signal Section, solved the sample message. When Commander Milo F. Draemel, the officer in charge, sent Hebern the solution, he came at once to Washington and showed the Navy his machine, filing his first rotor patent while he was there. The Navy had been looking, a director of naval communications later recalled, for "something radically better [in secret communications]. Something automatic came into our minds, and it had been in the back of our heads for some time. Along came Mr. Hebern from the West Coast with the Hebern machine. He made one, as I recall, and we were very thrilled when he showed us what it could do. ... I remember we wanted to get some right away for the whole Navy."

Hebern had, in 1921, incorporated Hebern Electric Code, the first cipher machine company in the U.S., and with this kind of encouragement from the Navy, and believing—rightly—that his new rotor device was the cipher machine of the future, he began selling shares in his firm to raise capital. Since it controlled scores of patents in the United States and abroad, not only on the cipher machine but on such other pioneering devices as electric typewriters and directional indicators for cars, he had no trouble selling about $1,000,000 worth of stock to 2,500 shareholders, mostly from Oakland, where he then lived. But he overexpanded, building a grandiose factory, and in 1926 Hebern Electric Code, Inc., went into bankruptcy.

Hebern refused to give up. Pinning his hopes on the Navy, he incorporated the International Code Machine Company in Reno, Nevada. Things started to look up in 1928 when he sold four five-rotor machines to the Navy at $750 for each machine and $20 for each rotor. Hebern and a handful of employees had built them by hand, and he himself then drove them to the 12th Naval District Office in San Francisco.

[Codebreakers 208.jpg]

*Edward Hebern's "Electric Code Machine," U.S. Patent 1,683,072. Rotors are 75a-e; plates, IS, 20, 21; the output letters glow behind the imprinted windows 37*

One machine stayed there; the others were sent to the Navy Department and to the commanders in chief of the United States Fleet and the Battle Fleet for field tests. The Navy wanted to determine their mechanical reliability rather than their cryptographic capabilities, which

were regarded as satisfactory, even though Friedman had made a cryptanalytic breakthrough and solved the first rotor system. During 1929 and 1930 these machines handled a considerable portion of the Navy's official high-command communications. Things looked even better for Hebern in 1931, when the Navy purchased 31 machines for $54,480. These were not experimental machines, but were issued to the more important flag officers as the top cryptographic system in the United States Navy. In 1934, Hebern, who was continually trying to improve his machines, submitted one that proved a complete failure. The officer who had dealt most with him, Safford, was on sea duty, and some Navy man who did not know Hebern sent him an abrupt and discourteous letter, discontinuing business with him. As Safford later put it, "They pulled the rug out from under Hebern and were not even polite about it."

That virtually ended Hebern's chances, for although his machines were still in service, when they wore out in 1936 after carrying heavy loads of traffic they were replaced by another, non-Hebern cryptographic system. Interestingly, the Hebern machines themselves were renovated and sent to shore stations, where some remained in use until 1942. Two were, in fact, captured by the Japanese during World War II.

During this time, Hebern was living on income from properties left by his wife's sister. He continued to improve his machines and to take out patents, despite the setback of losing a patent interference case against International Business Machines in 1941. In 1947, convinced that the armed forces had used his basic ideas throughout the war without compensating him for them, he filed a claim of $50,000,000 against the three services. In the six-year period that this remained entangled in bureaucratic red tape, Hebern died. He was 82, and had suffered a heart attack on February 10, 1952, while trying to lift a box that was too heavy for him.

Early in 1953, the departments of the Army, Navy, and Air Force rejected his claims, and a few months later his estate sued the government for the $50,000,000. On the basis of legal technicalities, the United States Court of

Claims limited the period of recovery to 1947-1953 and the infringement question to the exceedingly narrow one of a particular dog arrangement for turning the rotors. Ignored was the basic question of whether the armed forces had adopted the rotor principle from Hebern and used it without just compensation in hundreds of thousands of high-security machines in World War II and in the cold war—which they had unquestionably done. Ignored were the ethics of having obtained Hebern's best developmental efforts on the implied promise of large production contracts, which were awarded instead to the Teletype Corporation.

The government, taking refuge from the spirit of justice in the letter of the law, fought to keep from giving him a penny. In 1958, it finally settled for the pittance of $30,000—and not out of a sense of fair play, but because it feared that the court's sense of right would compel it to bare some cryptographic secrets. The payment was disproportionate to Hebern's contribution, which was worth, not $50,000,000, to be sure, but $1,000,000 at the least. Hebern deserved better. His story, tragic, unjust, and pathetic, does his country no honor.

Three others independently invented the rotor during the immediate post-World War I years. A Dutch engineer, Hugo Alexander Koch, 49, viewed the system most comprehensively, pointing out in his patent that steel wires on pulleys, levers, rays of light, or air, water, or oil flowing through tubes could transmit the enciphering impulse as well as electricity. A German, Arthur Scherbius, produced a machine called the Enigma. It failed commercially during the 1920s but became the standard cipher machine for all three armed forces when Hitler rearmed Germany in the 1930s. A Swedish inventor, Arvid Gerhard Damm, patented a cumbersome mechanism that seems never to have been built. The company that he founded likewise had at first no commercial success. But a young man, son of one of the investors in the firm, changed all that.

Boris Caesar Wilhelm Hagelin, born on July 2, 1892, in the Caucasus, where his father was working, studied for three or four years in St. Petersburg, then returned to Sweden and was graduated from the Royal Institute of Technology in Stockholm in 1914 with a degree in mechanical engineering. He worked six years for ASEA,

Sweden's General Electric, and one in the United States for the Standard Oil Company (New Jersey). In 1922, his father put him into the Damm firm to represent his investment.

Three years later, while Damm was in Paris, young Hagelin learned that the Swedish military was considering buying the Enigma. He simplified one of the Damm mechanisms. The Swedish Army liked it, and, in 1926, placed a larger order.

On the verge of success, Damm, early in 1927, died. Aktiebolaget Cryptograph, which was in poor financial shape but which had a big order in its pocket, was purchased at a good price by the Hagelin interests and reorganized as Aktiebolaget Cryptoteknik, 14 Luntmakare-gatan, Stockholm. Boris Hagelin ran the firm. He saw that printing cipher machines were faster, more accurate, and more economical in terms of manpower than indicating mechanisms like the Enigma, which lit bulbs to indicate plain- or ciphertext letters. To the army machine he added a printing mechanism. The whole apparatus weighed 37 pounds, operated at 200 characters a minute, and could be carried inside a case about the size of an attaché case.

This was the most compact printing cipher machine available in 1934, when the French general staff asked Hagelin for the impossible: a pocket-sized cipher machine that would print the ciphertext and so permit one-man operation. He first whittled a piece of wood that would fit into a pocket to mark the limits of his dimension. While trying to concoct a mechanism that would fit inside such space and also produce an effective cipher, he bethought himself one day of a construction that he had conceived three years before for the inventors of a vending machine. It was an adding device that would accept different amounts of money, and it consisted of bars arranged in a cylindrical cage with lugs projecting from them in rows. There were 10 lugs in one row, 8 in the second, 4 in the third, 2 in the next, and 1 in the last; by combining these rows in various ways any number from 1 to 25 could be produced. This was just what he needed. The inventors had given him the rights to it when they could not pay for the prototype that he fabricated. He now adapted it so that the rows would shift a cipher alphabet to any one of 25 positions, thus giving a plaintext letter any one of 25 ciphertext equivalents. And to produce the combinations

I

of numbers for these shifts, he could employ the keywheels with the variable number of projecting pins that he had used in his Swedish army machine.

Hagelin shrank the device to 6 X 4V& X 2 inches— smaller than the base of a standard telephone set—and to under three pounds, or about the weight of a dictionary-sized codebook. To operate it, the encipherer, after first setting the key elements, twirled a knob at the left to the plaintext letter, and revolved a handle at the right. The mechanism spun, and a little typewheel printed the output on a gummed tape. Hagelin even managed to have it print the ciphertext in five-letter groups and the plaintext in normal word-lengths (by using a rare letter as a word-spacer). Its speed averaged 25 letters per minute.

In essence, it is a gear with a variable number of teeth. These turn a cipher alphabet through as many positions as there are teeth for that particular encipherment. The various parts of the mechanism interact to produce an incoherent running key with a very long period. Moreover, it proved exceedingly rugged, and this plus other operational advantages and the ease of changing the key largely overcame its mediocre security, which resulted from its use of a normal instead of a mixed alphabet as the cipher alphabet.

From a purely mechanical point of view the device is an absolute marvel. Hagelin has engineered a mechanism that spouts an extremely long key from relatively few elements in an astonishingly compact format, which also permits of practically unlimited key changes. It is the most ingenious mechanical creation in all cryptography.

This was the Type c-36, and when the French saw it, they snapped it up. Their 1935 order for 5,000 machines proved the turning point in the firm's fortunes.

That same year, Hagelin began corresponding with American cryptologic authorities about the c-36. He went over himself in 1937, and again in 1939 when war broke out in Europe. Now the United States was considerably more interested. Friedman suggested improvements, and Hagelin returned to Sweden to incorporate them and to streamline the machine for mass production. On April 9, 1940, he was in his cabin in Dalecarlia when he heard a radio announcement that the Germans had invaded Norway. His wife told him that if he wanted to do anything with his machine in the United States, he ought to go there at once.

[Codebreakers 213.jpg]

*Boris Hagelin's* M-209. *1 Outer cover 2 Inner cover 3 A lug 4 Encipher-decipher knob, set at D for decipher 5 Paper tape 6 Letter counter 7 Indicating disk, on which input letters*

*are set 8 Reproducing disk, on which output letters are shown 9 Typewheel, which prints output letters 10 Windows to display keyletters on keywheels 11 Power handle 12 Cage disk, numbered for each slide-bar 13 A slide-bar, which moves left to become a tooth of the variable gear 14 Keywheel advance gear 15 Upper part of angled face of guide arm of keywheel 4; lugs in column 4 will strike it as cage rotates forward, driving slide-bars to the left 16 Pin for S on keywheel 4, in ineffective position 17 Keywheel 5*

"A normal visa was unobtainable," he has recalled, "so I induced the Swedish foreign office to send me as a diplomatic courier. My wife and I sent our luggage off in advance and took the train up to Stockholm. There we learned that the travel bureau had cancelled all trips to the United States, as the Germans had by now invaded France, Holland, and Belgium. We decided to take a chance and try to sail from Italy.

"With the blueprints in my briefcase and two dismantled ciphering machines in a bag, we boarded the Trelleborg-Sassnitz-Berlin express. Our luck held. We rattled right through the heart of Germany and arrived unmolested three days later in Genoa. That night the windows of our hotel were smashed—because we had innocently chosen to stay at the Hotel Londra and Italy was now at war with Britain. But we reached New York on the last outward-bound voyage of the *Conte di Savoia."*

This breathless escape proved worth it. The U.S. Army liked the machine, though it insisted on further tests. Hage-lin got 50 machines flown out secretly from Stockholm to Washington for final exhaustive trials. They passed, and after long contract negotiations, the Army accepted the improved device as its medium-level cryptographic system. Under the U.S. military designation of Converter M-209, the Hagelin machine served in military units from divisions down to battalions. In 1942, L. C. Smith & Corona Typewriters, Inc., began turning out about 400 olive-drab Hagelin machines a day (compared to its output of about 600 typewriters a day) in its 900-man factory at Groton, New York. More than 140,000 were produced. (Ironically, the Italian Navy also used it.) Hagelin's royalties ran into the millions of dollars. He became the first—and the only—man to become a millionaire from cryp-tology.

## 12. Duel in the Ether: I

SHORTLY AFTER NOON on the tense 31st of August, 1939, the last day of peace that the world was to know for six years, Swedish businessman Birger Dahlerus met with

Hermann Goring at the Nazi leader's large and richly furnished town house at 2 Leipzigerstrasse in Berlin. Dahlerus had been trying desperately to avert the onrushing cataclysm of war by flying between England and Germany as Goring's unofficial mediator. Britain had pledged to aid Poland if Hitler attacked her, and, in an effort to stave off actual warfare had proposed to both Germany and Poland that they negotiate their differences directly. At a few minutes past one, as Dahlerus and Goring were discussing the situation, an adjutant brought in a red envelope of the kind used for especially urgent affairs of state. Goring ripped it open. When he read its contents, he leaped from his chair and, striding angrily up and down, raged at Dahlerus that he had in his hands proof that the Poles were sabotaging every move toward negotiation.

After a few minutes he calmed down enough to tell the Swede what had been in the envelope. It was a telegram from the Polish government in Warsaw to its ambassador in Berlin. It was in code, of course, but the cryptanalysts of Goring's Forschungsamt, who had long ago cracked the Polish diplomatic code, had reduced it to plaintext at once, translated it into German, and sent a copy to Goring via messenger. The entire process had taken the communications-intelligence agency less than an hour.

At the" end of the telegram came a "special and secret message" to the ambassador: "Do not enter under any circumstances into any factual discussions...." To Goring this proved so conclusively that the Poles had no intention of negotiating in good faith that he copied the translation in his own hand for Dahlerus to show the British ambassador. The German Air Minister told Dahlerus that he was taking a great risk in doing this—he undoubtedly meant jeopardizing Germany's possession of the Polish code—but felt that Britain should know how faithless the Poles were.

In fact this was not a reason for going to war, but just another excuse to do so. The Germans were using Dahlerus as a cat's-paw, for at the very moment that Dahlerus entered Goring's home, Adolf Hitler was signing his "Directive No. 1 for the Conduct of the War." At daybreak the next morning German troops invaded Poland. And although the Forschungsamt solution of the Polish message had no role in that attack except to confirm the Nazis in their perfidy, it did demonstrate the keenness and efficiency of one of Germany's major intelligence weapons as she

I

embarked upon what she fondly thought would be her blitzkrieg of conquest.

The cryptanalytic service of the German Foreign Office was created early in 1919, apparently at the suggestion of Kurt Selchow, a 32-year-old former captain in the Army intercept service. Selchow became its administrative chief and staffed it with cryptologic acquaintances from the war. His organization was at first known as Referat I Z, the z section of Division I, Personnel and Budget, of the Foreign Office. It included both the cryptanalytic service (the Chifinerwesen) and the cryptographic (the Chiffrierburo), the latter twice as large as the former. Around 1936 a reorganization of the Foreign Office renamed *I Z as* Pers *z* (pronounced "pers-zed"), the z section of the Personnel and Administrative Division. The z meant nothing—the division did not have 26 sections—and it may have been chosen because it seemed appropriate to cryptology. Much later, Foreign Minister Joachim von Ribbentrop took the Chiffrierburo under his own office.

By 1939, Pers z had divided the Chiffrierwesen into two groups—one that dealt with ciphers, either as primary systems or as superencipherments, and that was heavily mathematical in personnel and approach; and one that dealt with codes and emphasized the linguistic.* Three senior cryptanalysts headed them—Rudolf Schauffler and Adolf Paschke as joint chiefs of the linguistic section, Dr. Werner Kunze as chief of the mathematicians. All were veterans of the military cryptanalytic bureaus that Germany had belatedly started in World War I; all joined the Foreign Office in 1919 when they were close to 30. Schauffler and Kunze participated in developing the one-time pad, the unbreakable cipher in pencil-and-paper form.

These three were chiefly assisted by three other old-timers, Erich Langlotz, the third inventor of the one-time pad; Ernst Hoffmann, who held the title of Counsel for the High Cipher Service; and Hermann Scherschmidt, a specialist in Polish and other Slavonic codes. All usually held the same rank of Regierungsrat that Kunze, Schauffler, and Paschke did. In 1933, when Hitler came to power, Pers z employed about 30 civil servants. As Germany re-

*This division carries into the practical sphere the distinction that codes operate upon texts linguistically whereas ciphers operate nonlinguistically.

armed, Pers z expanded, though slowly at first. Recruiting was subtle: prospective recruits did not know that they were being considered for the highly secret work of cryptanalysis. One woman, Asta Friedrichs, who had taught school in Bulgaria and knew that language, which Pers z needed, was simply asked if she would like to learn Serbo-Croatian and do some work involving it; she accepted, and not until after a probationary period was she told about the code-breaking. She began solving Serbo-Croatian codes, then some Bulgarian, then helped with others.

With the outbreak of war, Pers z's growth became explosive. Among the brightest of its new members was Dr. Hans Rohrbach, a 37-year-old mathematician who later became editor of the oldest mathematical journal in the world, the *Journal of Pure and Applied Mathematics.*

For several years, Pers z had been situated on the top floor of the library building just behind the Foreign Office main building in Berlin's Wilhelmstrasse. But by early 1940, it had burst out of these quarters. The mathematicians moved out first, into several flats in an apartment house at w-8 Jaegerstrasse that had been entirely taken over by the Foreign Office. Their departure relieved the crowding in the original office only temporarily, and soon the linguistic codesolvers found new offices, first in an anthropological museum, where they were surrounded by artifacts from Siam, and then in Dahlem, a suburb of Berlin. Here some worked in a garden apartment on a street called ImDol, some in a nearby girls' boarding school, where they were joined in 1943 by the mathematicians. The combined group, the Chiffrierwesen arm of Pers z, called itself the Sonderdienst Dahlem ("Dahlem Special Service"). While there, during the middle period of the war, it consisted of about 200 staff members—20 to 25 mathematical crypt-analysts, probably the same number of linguistic crypt-analysts, the rest clerks and support staffers. Later it grew to 300.

Heavy bombings—the workers had to spend nearly every night in air-raid shelters—forced still another move in the summer of 1944. The linguistic branch moved 150 miles southeast to Hirschberg in Silesia, where they installed themselves in another school; the mathematicians moved to the nearby town of Hermsdorf. The odyssey of Pers z did not end even there, however. In February, 1945, the advance of the Russians compelled each group to move

about 150 miles west. The mathematicians evacuated to Zschepplin Castle, near Eilenburg, about 80 miles south of Berlin. The linguists, joined by a few mathematicians to strip current superencipherments, moved into a wing of Burgscheidungen Castle near Naumburg, northwest of Wiemar. Here, as wartime guests of the Count von der Schulenburg and his five daughters, the 90 cryptanalysts, some with their wives, lived and worked amid art treasures and ancient furniture, handicapped by the almost total lack of liaison with the mathematicians, about 50 miles away.

The ever-present problems of security added to the difficulties of Pers z. Ink was not permitted because it required blotting paper. Each night all papers had to be locked away. Waste paper had to be burned, and the ashes broken up to make sure that no cinder would float away. Later Pers z got a machine to shred the paper before it was incinerated. None of the codesolving groups was allowed to know what the others were doing—but these artificial barriers dissolved in the camaraderie of the Dahlem bomb-shelter.

Security also meant political security, and even before the war the Nazis planted a spy in Pers z to watch for any signs of anti-Hitler activity. In 1942 Selchow became a Nazi. He took the honorary rank of Sturmfiihrer, which gave him access to three of four cars. The next year he became an Obersturmfiihrer because this gave him "a certain authority with the drivers." However, he insisted, he never wore the uniform. Among the cryptanalysts, Paschke, Schauffler, and Kunze, at least, also joined the Nazi party.

The cryptanalysts' raw material was intercepted by either military radio stations or the post office telegraph bureau. In Silesia, it came in by courier about noon. Most of the diplomatic messages bore address and signature, so few traffic-analysis problems of discovering language, cryptographic family, and the like, arose. The cryptanalyses required enormous volumes of text and corresponding quantities of statistics. The army of clerks, mostly women, compiled these, but it usually paid the cryptanalysts to work up a few statistics themselves. The solutions took a heavy toll of nervous energy. "You must concentrate almost in a nervous trance when working on a code," Miss Friedrichs recalled. "It is not often done by conscious effort." The solution often seems to crop up from the subconscious.

The subconscious got considerable help, however, from an information group headed by Pastor Joachim Ziegen-

riicker. The group collated information from radio broadcasts, Foreign Office memoranda, Allied newspapers (it read *The Times* throughout the war), and the Pers z output so that, as Miss Friedrichs said, they could give the answer when the cryptanalysts asked them "Who beginning with w spoke with somebody ending with *n* in a place with a kind of *po* on Thursday?"

More help came from the financial bonuses that kept up the codebreakers' knowledge of foreign languages. The amount depended upon the difficulty of the tongue; nothing was paid for English and French, which they were expected to know anyway. The codebreakers had to take an examination in the language every four years to prove their continued competence, and many of them learned four languages, taking an examination each year and brushing up at the local Berlitz school for a month before the test. Pers z had experts in the language of almost every country large enough to maintain a diplomatic corps. One Olbricht attacked the difficult problems of breaking Chinese codes. A man named Benzing took such delight in the Turkish language and Turkish cryptanalysis that his confreres regarded him as a veritable Turcomaniac.

The cryptanalysts received some of their greatest help from robots—mechanisms that speedily performed some of the highly repetitious tasks required, or that simplified the handling of many items. Many were tabulating machines that used punched cards in ordinary ways. But many others were assembled out of standard parts for special purposes by Hans-Georg Krug, a former high school mathematics teacher who possessed a positive genius for this sort of thing.

These Pers z robots helped solve codes of France and Italy, both of which used at times four-digit codes with additive superencipherments. One English code, however, remained invulnerable, because the 40,000-group length of her additive key prevented enough material from accumulating. At the start of World War II, most countries probably employed the additive system of enciphered code in a hierarchy of codes for their foreign services. Germany herself did, using sometimes a four-digit, sometimes a five-digit code, only her additive was the one-time pad. Despite all the mechanical help, however, solution of most codes came right down to pencil-and-paper work by individual cryptanalysts.

Such was the solution of the superencipherment of the Japanese TSU diplomatic code—the columnar transposition with blank spaces in the transposition blocks that American cryptanalysts called the K9 transposition to the j!9 code. The Japanese embassy in the Soviet Union began relying heavily on this code in October of 1941, when the Soviet government moved its capital eastward from threatened Moscow to Kuibyshev. The diplomats had to stay close to the seat of government, and the Japanese may have junked their heavy cipher machine instead of moving it, using their paper codes instead. Pers z made its first break by spotting two messages which had patches of identical letters separated by nonidentical sections. Deducing that these differing portions represented the same placode text, the cryptanalysts compared the two messages until, in a single afternoon, they found a transposition and blank arrangement that yielded the same texts in a form that resembled legitimate codewords. In one of their greatest technical successes, the mathematical cryptanalysts cracked the approximately 30 transposition and blank patterns; the linguists read the code, and the subsequent solutions pro vided the Germans with information about Russian war production and army activities.

[Codebreakers 220.jpg]

*Pers z solution of an encoded message of Robert Murphy to the State Department dealing with highly secret negotiations with General Weygand in North Africa in 1941*

Pers z was an old hand at reading American codes. It had long studied the American superencipherment. The codewords were only of the cucuc and cuccu types (c = consonant, v = vowel); to encipher, the code clerk split them into a single consonant and two cu or uc groups, then replaced these segments with substitutes from the appropriate tables. This superencipherment left the cucuc and cuccu configuration of the codegroup unchanged, and this regularity enabled the Pers z mathematicians to break first into this original system and, in 1940, into a modification of it._ Ironically, changes of superencipherment within a message, intended to provide greater security, furnished the German cryptanalysts with isomorphic repetitions that helped them reconstitute the superencipherment substitution. With the superencipherment stripped off, the linguistic group solved a big 72,000-group code with not too much trouble. Dr. Hans-Kurt Miiller was instrumental in this; he had an uncanny gift for seeing the outlines of the whole plaintext in the murk of the partial solutions. Miss Friedrichs assisted.

They were greatly helped in their work by their knowledge of the activities of diplomat Robert Murphy, who in 1941 and 1942 was in North Africa, handling delicate negotiations with the Vichy French and paving the way for the Allied invasion of North Africa. Murphy insisted upon using the State Department codes to preserve his autonomy, even though American officers in Eisenhower's command pointed out their insecurity. He was certain that the Germans had not broken his codes. In fact, however, the Pers z cryptanalysts had broken them enough to recognize the groups meaning *For Murphy* or *From Murphy* that recurred at the head of so many telegrams. "We knew what he was interested in, and this gave us clues," Miss Friedrichs said. These rapidly helped complete the solution of the big code. Murphy's communications so facilitated her work, she said, that when she saw him drive by one day after the war while she was interned in Marburg, "I wanted to stop him and shake his hand."

Thus, as early as August 12, 1941, the state secretary of the Foreign Office could hand to von Ribbentrop fully solved copies of Murphy's telegrams of July 21 and August 2. The first reported that Murphy had transmitted Roose-

velt's views on French North Africa to General Maxime Weygand, commanding there. The second transmitted a Weygand aide's request for an American promise of military assistance. The Nazis knew Weygand was no friend of theirs, but it was not until they had what a Vichy source called "documentary proof" of his dealings with the United States that they forced Vichy to dismiss him. Thus the solution of an American diplomatic code cost the United States much valuable time and work that it was forced to recommence with the new leaders of French North Africa, and it may ultimately have prolonged the war and cost the lives of American soldiers who fought in that theater.

As the war progressed, the State Department gradually took the old solved codes out of service and replaced them with new cryptosystems. It thus choked off the German sources of information. To get them flowing again, Pers z launched, in 1944, a major effort to break the M-138. This top State Department system was a Jefferson cylinder in strip form—the alphabets are "peeled" off the disks and stretched onto paper strips. The work was primarily mathematical, with Hans Rohrbach, a 37-year-old doctor of mathematics, playing a leading role. Rohrbach and Miiller first divided the messages into "families" enciphered with the same strip arrangement, using repetitions as family resemblances. This meant that, in a given family, the first strip was always the same, the second was always the same, and so on. Stereotyped beginnings gave the crypt-analysts many plaintext assumptions—Miiller was as adept at spotting words here as with the code. On each strip, the plaintext stood an unknown distance from the ciphertext. By comparing many such equivalents, both within a single strip and with the help of information from neighboring strips, the cryptanalysts mapped the letters on the strips to reproduce the original alphabet. Collaboration among the half-dozen cryptanalysts was extremely close. Each man looked after his own families, but they conferred frequently so that each could try on his own sequence of strips the possibilities found by others. Helping them in their work was a mechanism that moved the strips up and down to align them quickly. Eventually Pers z recovered all the M-138 strips and read nearly all the messages. But by then they had lost much of their intelligence value, and any hopes that the solution would help in the future vanished when the strips were changed.

The codes of small countries are usually simpler to solve than those of large, and not only because of intrinsic qualities as smaller code size and fewer codes and additive tables. Their personnel is less well trained, and so they often ask for repeats if, as happens more often than with major powers, they cannot decode a message. Moreover, not having the courier services or communications of larger and richer countries, they cannot get new codes to distant outposts as often as the large countries and so continue using the older codes too long. While their messages usually do not contain the crucial portents of those of great powers, their diplomats are sometimes well situated and can provide information of value. Yet even these small nations sometimes seem to have a feel for knowing when their codes are broken. "You just get to a point where you are reading a good part of the traffic when one morning you come in and it's all changed," said Miss Friedrichs.

The Pers z solutions, typed up, went to Selchow. He submitted them to the state secretary of the Foreign Office before Ribbentrop became Foreign Minister, and afterwards to both the state secretary and the Foreign Minister's office, at Ribbentrop's order. Those for the Fiihrer were marked with a green "F." He did not always see them, since Ribbentrop did not dare give him bad news. Those that he did see, he did not always appreciate. Across the face of one long dispatch that gave considerable information on agricultural conditions in Russia, which bore importantly upon military possibilities, Hitler scrawled "Kann nicht bir stimme" ("This cannot be"). Nazidom preferred its own lies and. propaganda to unpalatable truths, and so, as Miss Friedrichs said, "Even if we had a plum, it was not considered as one."

In April of 1945, the American front engulfed the crypt-analysts at Burgscheidungen Castle and swept past. A few days later, Haskell Cleaves, a Signal Corps officer from Maine, discovered what they were doing. Headquarters sent out a mixed commission of American, British, and French experts to interrogate them. On May 8, while the world was celebrating V-E Day, 35 of them were flown to London for interrogation. For the cryptanalysts of the German Foreign Office, the war had ended.

What had they accomplished? They had achieved some remarkable technical successes, and for some that was enough. Kunze and the other mathematicians usually lost

interest in a problem after its cryptanalytic difficulties had been surmounted. Even the codebreakers who were interested in their influence on their country's policy could rarely learn anything about it: the diplomats seldom told them, and Selchow stood between them and the users. Moreover, the effects were diffused over many messages, commingled with other sources of information, distorted by Nazi preconceptions, so that it was virtually impossible to single out cryptanalyzed information as critical in a specific event. Finally, and most important, Germany lost the war, reducing all the Pers z efforts in the final analysis to nullity. "As I am accustomed to say," said Schauffler, "a bridge builder can see what he has done for his countrymen, but we cannot tell whether our life was worth anything."

Yet they read the secret communications of the British Empire, Ireland, France, Belgium, Spain, Portugal, Italy, the Vatican, Switzerland, Yugoslavia, *Greece,* Bulgaria, Rumania, Poland; Egypt, Ethiopia; Turkey, Iran, China, Japan, Manchukuo, Thailand; the United States, Brazil, Argentina, Chile, Mexico, Bolivia, Colombia, Ecuador, Peru, the Dominican Republic, Uruguay, Venezuela. Not every code of every country was always read, but the solution of the codes of 34 nations of the earth suggests that, whether or not the Pers z cryptanalysts' life was "worth anything," the reckoning cannot involve whether they had done their duty. That they had.

In the nightmare totalitarian jungle that was Nazi Germany, the bigwigs of National Socialism consolidated their positions by building up personal power structures. Extra power could come from the knowledge obtainable through intercepting communications. Thus it was that a few weeks after Hitler appointed Hermann Goring as Air Minister in his new government in 1933, the fat ex-air ace established an eight-man unit in his Air Ministry to do as much intercepting as possible. He called it the Forschungsamt ("Research Office"), but its research was highly specialized. Apparently attached to the minister's office, it bore no relation either to the research division of the Luftwaffe's technical office or to the Luftwaffe's own military intercept and cryptologic unit.

Goring installed the Forschungsamt in a requisitioned building on the Behrendstrasse, Berlin, but moved it at the end of 1933 to the Hotel am Knie in the suburb of Chariot-

tenberg. He named as its first chief an old friend and loyal party member named Hans Schimpf, a former naval lieutenant who had once served as liaison between the Army and the Navy cryptologic organizations. In 1934 the unit did exactly what Goring expected it to do when it supplied him with information that helped him win Hitler to his side in the first great power struggle of the Third Reich— that between Hitler's oldest friend and closest associate in the Nazi movement, the homosexual Ernst Roehm, on the one hand, and Goring, Heinrich Himmler, head of the S.S. and the Gestapo, and the Junkers on the other. Roehm was shot, and soon thereafter Schimpf suffered the same fate, presumably because he had done his job so well that he knew too much. Goring replaced him with Prince Christoph of Hesse, younger brother of Prince Philip of Hesse, one of Goring's friends since the late 1920s. Christoph, then in his mid-thirties, was the fourth and youngest son of the Landgrave of Hesse, former ruler of that principality and a member of one of the oldest traceable families in Christendom (to Charlemagne). Christoph became a ministerial director in the Air Ministry and also had the title of Oberfuhrer of the S.S. He died in Italy in 1941 and was replaced by one of the original members, Gottfried Schapper.

The Forschungsamt tapped telephones, opened letters, solved encoded telegrams. Its reports were called Braune Blatter ("Brown Sheets"). A typical one, of March 19, 1945, which was passed to the economic division of the armed forces, reported that on March 14 the Swiss political department informed the Swiss embassy in Lisbon about an agreement reached with the Allies concerning railroad operations from southern France. The Forschungsamt also recorded the conversations of Goring and Hitler. These were passed to the appropriate government department for action or reference, if necessary. In its most famous case, it transcribed 27 conversations from Goring's office with various officials in Rome and Vienna that settled Austria's fate in the hours before the Anschluss. Ironically, one of those whose subservient words to an overjoyed Hitler were recorded for posterity was Prince Philip, emissary of the Fiihrer and brother of the chief eavesdropper.

Christoph's membership in the S.S., or Schutzstaffel ("Protection Staff"), the notorious blackshirted strong arm of the Nazi party, pointed to a close relationship between the Forschungsamt and the S.D., or Sicherheitsdienst

("Security Service"), the branch of the S.S. that served as the ideological watchdog for the Nazis. The S.D., for example, determined who voted the wrong way in German plebiscites by numbering the back of the ballots with milk, a simple effective secret ink. Its efforts were primarily internal, and since private citizens, even conspirators, seldom use complicated code or cipher systems, its crypt-analytic organization—if it even had one—was small and nameless. This is not to say that the S.D. was not interested in other people's conversations: it probably did its share of telephone tapping and mail opening.

After 1936, the S.D. extended its watchdog duties from just the party to the government as well, with a domestic branch and a foreign branch that would nullify dangers before they could be launched against the sacred soil of the German Reich. Probably the S.D. also broadened its communications activities somewhat. It filched a diplomatic telegram here and there, and listened in to diplomatic telephone conversations, even one, on May 7, 1940, between Prime Minister Neville Chamberlain of Britain and Premier Paul Reynaud of France—Chamberlain and Reynaud could certainly be considered enemies of Germany and the Nazi party. But the S.D. probably got most of the external communications intelligence that it needed from the Forschungsamt, which was quite as interested as the S.D. in preserving the Nazi regime.

Himmler headed the S.S. as a party official; as a government official he headed the two Reich police organizations: the Gestapo, which handled political crimes, and the Kripo, or Kriminalpolizei, which dealt with ordinary crimes. Both had communication intelligence sections, but, as with the S.D., these probably concentrated primarily on telephones and mail and had but little cryptanalysis to do.

In 1939, the party and government police organizations were merged as the R.S.H.A., the Reichssicherheitshaupt-amt ("Reich Central Security Office"). The Gestapo became Amt IV of the R.S.H.A., the Kripo Amt V. The government domestic watchdog branch of the S.D. evolved into the R.S.H.A. Amt III, Domestic Intelligence, and the foreign branch into Amt VI, Foreign Intelligence. Amt VI was charged with the production of secret information about enemy countries.

It apparently directed its thoughts mainly to the more traditional methods of gathering such intelligence. But

shortly after the Anschluss, Walter Schellenberg, a young S.D. official, seized the files of the Austrian secret service and found that among the most interesting documents were those on cryptanalysis. This find may have soon thereafter recalled to the mind of Wilhelm Hottl, a youthful Austrian staff member of the new R.S.H.A., the World War I deeds of the Austro-Hungarian cryptanalysts, which General Max Ronge had detailed in an exciting book. Hottl discovered that General Andreas Figl, former head of the Austrian Dechiffrierdienst, had been arrested by the Gestapo in 1938. Hottl got Heinz lost, then head of Amt VI, to free Figl and to install him as an instructor in cryptology in a villa in the Wannsee section of Berlin. Here he passed on his experience to a new generation.

But such training takes time, and any intelligence that the R.S.H.A. obtained from communications continued to come to it from other sources. It seized an occasional plaintext telegram and somehow acquired a one-part Spanish code and used it to read intercepts. It also was granted what must have been the first opportunity in history to get codes wholesale. Yamato Ominata, Japan's intelligence chief in Europe, offered to deliver the Yugoslav general staff and Turkish, Vatican, Portuguese, and Brazilian codes for 28,000 Swiss francs, or about $20,000. The offer may well have been accepted, for all those codes were read at one time or another by various German agencies.

In addition, the R.S.H.A. depended upon the military and the Forschungsamt for communications intelligence. Thus, in the autumn of 1941, Schellenberg, who had become deputy chief of Amt VI, asked Reinhard Heydrich, head of the whole R.S.H.A., to contact both the Forschungsamt and the military. Schellenberg wanted them to concentrate their intercept posts and cryptanalysts on Vichy and Belgrade traffic for some information he needed. At about the same time, Heydrich called the chief of the Wehrmacht signal organization and asked him to send Schellenberg any information about American-Japanese negotiations that he might obtain.

Himmler disliked such dependency and in March of 1942 he sent Schellenberg to Goring's beautiful country house, Karinhalle, to urge that the Forschungsamt be incorporated into Amt VI. Goring greeted him in a Roman outfit, toga, sandals, and all, carrying his Reichmarschal's baton, and, after hearing Schellenberg, said vaguely, "Well, I will have

a word about it with Himmler." Nothing happened, of course, and Schellenberg, who at this time became head of Amt VI, set up a well-funded department, to carry out research in secret communications including invisible inks and microfilms as well as cryptography and cryptanalysis. Figl may well have been the nucleus of this group. It may have provided the digraphic cipher—ten tables 26 X 26, one of which was selected to encipher each message— that one R.S.H.A. radio net was using much later in the war. This system may have been adapted from the Army, which at one time used digraphic substitution as a field cipher. For internal communications, the R.S.H.A. used cipher machines supplied by the military.

The new department did not, in any event, produce a great deal of communications intelligence, for Schellenberg continued to get most of his from the outside. Starting in 1942, he said, "Every three weeks or so I gave a dinner party at my home where the technical heads of the three services, Defense Ministry, Post Office [which unscrambled transatlantic telephone conversations], and Research Stations [Forschungsamt] discussed new developments and helped each other with their problems.* These meetings were perhaps more than any other single factor responsible for the high standard of the scientific and technical side of my service. It was the cooperation and interest which these people showed to me personally which made most of my success in Secret Service operations possible"—an unexampled acknowledgment of indebtedness to communications intelligence by a cloak-and-dagger man.

The R.S.H.A. repaid some of this generous help with the products of the greatest spy coup of World War II— Operation Cicero. "Cicero" was Elyesa Bazna, an Albanian working in Ankara as the valet to Sir Hughe Knatchbull-Hugessen, British ambassador to neutral Turkey. Bazna had taken wax impressions of the keys to the black dispatch box which Sir Hughe kept beside his bed for the secret papers that he liked to pore over late at night. The valet would open the box, photograph the documents, and sell the rolls of film to the R.H.S.A. agent in Turkey, L. C. Moyzisch provided the Germans with information about Russian war production and army activities.

*No Pers z representative appears to have attended—probably a reflection of the high-level personal dislikes and power struggles between Goring and Himmler on the one hand and Ribbentrop and the military on the other. At one point Goring tried to bring Pers Z within the ambit of the Forschungsamt.

[Codebreakers229.jpg]

*Encipherment table* H-1 for a *diagraphic cipher of an R.S.H.A. radio net in Norway*

The documents consisted largely of cables to Sir Hughe. They were of the highest importance—reports of Stalin-Roosevelt-Churchill conversations, for example. But when this information began streaming into Berlin in November and December, 1943, Hitler and other top officials refused to believe that it was genuine. "Too good to be true," Ribbenthrop told Moyzisch. The fact is that he did not want to read therein the impending doom of the German Reich.

The messages, which bore date-time notations, could help in breaking the British diplomatic codes, and though Pers Z would seem to have been the logical recipient, Schellen-berg gave the photographs to his communications-intelligence friends in the military. They cooperated fairly closely with Pers Z, however, and they probably passed the material to it. Pers z may also have gotten copies from Ribbentrop. Kunze and Paschke both saw Cicero documents and were unimpressed. For the British were by then superenciphering their most secret messages in a one-time pad. Though the Cicero messages may have contributed to the solution of some lesser British systems and so helped produce some minor information, they could not make possible the recovery of the one-time keys of any other messages. Operation Cicero, so complete a success in one sense, was thus an almost total failure in another.

At about this time, Hottl, the young man who had discovered Figl, became, at age 28, the head of Amt VI E— the Amt VI section for southeast Europe. He soon grew friendly with Hungarian Army intelligence, whose chief one day showed off his communications-intelligence unit. The Hungarians did indeed have a fine organization, and it very much impressed Hottl. He thought that it did relatively more with its poor resources than did Pers z, the Forschungsamt, the German military cryptanalysts, and the police eavesdroppers all put together. In the middle of 1944, he convinced the pro-Nazi Hungarian Premier, Andor Sztojay, to have the unit furnish him with its results. The unit's commander, Major Bibo, who lived only for his work, agreed to concentrate on the traffic that Hottl wanted when Hottl promised him more men, better equipment, and extra money.

Hottl went from room to room in Bibo's offices and picked out the choicest of the copious solutions. A few days later, he laid the sheaf before Schellenberg and said: "Please read this, and if you would like to have it regularly, give me a credit for the first 100,000 Swiss francs." But Schellenberg feared that Hitler, who distrusted the Hungarians because of their marked lack of enthusiasm for being an Axis partner, would not like the idea if he heard of it. He gave Hottl only a nominal sum. But Hottl wangled the francs out of the R.S.H.A. financial wizard, Friedrich Schwend—not too difficult a task, since the money was bogus.

Within six months, the unit exceeded even Hottl's sanguine hopes by reading a goodly portion of the secret radiograms of embassies in Moscow. Figl seems to have joined it and become one of its star cryptanalysts, performing some minor miracles in his room with pots of black coffee and packs of cigarettes whenever the unit was stumped. Bibo's interceptors and cryptanalysts had become the R.S.H.A.'s first major source of its own of foreign communications intelligence. It could read some American and British messages, especially in 1945, when it acquired a cryptanalyst "who could sift the unimportant from the important with the sureness of a sleep-walker." It read almost all the radio traffic of the Turkish embassy, learning that Stalin deeply suspected his Anglo-American allies and feared that they might conclude a separate peace with Germany. The reports of the Turkish military attache[1], Hb'ttl was told by General Alfred Jodl, chief of the Wehrmacht operations staff, contained the most valuable information about Russia that the high command then had. By this time, about the end of 1944, the advancing Russians forced the unit to retreat from Budapest to the Odenburg hills and, three months later, to an Alpine redoubt. These disruptions did not choke off the flow of intelligence, which ended only when the war did.

"I do not want to exaggerate the importance of what we achieved, although in this one year of my collaboration with the Hungarians there were at least a hundred successes such as seldom fall to the lot of a Secret Service working in the ordinary ways," Hottl wrote. His impressive tribute, which independently seconds the praise that Schellenberg offered to other cryptanalysts,' confirms the overwhelming supremacy that communications intelligence attained in both quantity and quality over almost any other form of secret intelligence in World War II.

Germany's armed forces had their own agencies for cryptanalytic intelligence.

Of these there were four: one in the Oberkommando der Wehrmacht for the armed forces as a whole, and one each for the high commands of the Army (O.K.H., or Oberkommando des Heeres), the Navy (O.K.M., or Oberkommando der Kriegsmarine), and the Air Force (O.K.L., or Oberkommando der Luftwaffe). All but the naval unit traced back to an intercept service established in the Army in

1919 by First Lieutenant Erich Buschenhagen, who had worked in radio intelligence in the war. He called it the "Volunteer Evaluation Office."

This unit stepped up its activities as Allied post-Versailles supervision waned in the 1920s. Part of its work consisted of picking up press association messages and news broadcasts and distributing a digest of them to government officials. By 1926, it had intercept stations in six major cities of Germany. In 1928, it began following the military maneuvers in which neighboring countries were once again engaging. It sneaked its intercept units into the demilitarized zone along the Rhine by disguising them as technicians for the German broadcasting or postal organizations. Much of its success resulted from traffic analysis—in 35 of the 52 major maneuvers between 1931 and 1937, the foreign forces were reconstructed completely. But it also solved some cipher systems.

When in 1934, Hitler pointed Germany toward its eventual war of revenge and conquest, he swelled the ranks of the armed forces and intensified military activities. But though the cryptologic agencies likewise grew in size, they did not necessarily grow in effectiveness. There were too few specialists in this recondite field to fill the need created by the proliferating military and party organizations. Some of the Army cryptanalysts were siphoned off to serve in the Forschungsamt, others, the Luftwaffe. Some of the intercept people moved over to Josef Goebbels' Ministry of Propaganda, where their news-eavesdropping could help. About 1937, the O.K.W. created its own communications and cryptologic staff, thereby draining off more of the experts and further splintering the effort in the field. These new agencies were staffed by World War I veterans who were now rejoining the German Army; most had been officers in the signal corps but had no great exprience in or aptitude for intercept or cryptologic work. By mid-193 9, the German communications-intelligence services had 18 times as many people in them as they had had in 1932, but useful results had in no way kept pace.

Six days before Hitler fell upon Poland, Major General Erich Fellgiebel, 52, who had been in communications since he joined a telegraph battalion upon enlisting in 1905, was named head of the O.K.W. communications organization. His title was Chef, Wehrmachtnachrichtenverbindungen

("Chief, Armed Forces Signal Communications"), or Chef W.N.V. His superior was the O.K.W. chief, Field Marshal Wilhelm Keitel, whose only superior was Hitler. Keitel wrote in FellgiebeFs fitness reports: "In his field a pronounced leader type with foresight, a gift for organization, full energy and dedication. ... In his attitude towards National Socialism an inclination to unconsidered over-criticism. ..." The W.N.V. supervised communications, including communications security, and intercept operations;* it served as a kind of staff, an advisor and controller, for the service branches that largely operated the communications and intercept networks for the Army, Navy, and Air Force, much as the O.K.W. itself advised and directed the service commands.

Under the Chef W.N.V. came the Amtsgruppe W.N.V. Its chief was Major General Fritz Thiele, 48, a close colleague of Fellgiebel's who had previously headed the O.K.H. communications and intercept organization. He became Chef, Amtsgruppe W.N.V. the day the war began. The unit comprised radio and wire branches, which maintained communications between the headquarters of the three armed forces high commands, a technical equipment office, an administrative office, and the Chiffrierabteilung ("Cipher Office"), usually abbreviated "Chi." Colonel Siegfried Kempf assumed command of Chi on the same day that Fellgiebel became Chef W.N.V. Then 43, he was a career communications officer, a martinet disliked by his subordinates. He was succeeded in October, 1943, by Colonel Hugo Kettler, 48, who had had considerable intercept experience and who brought out the best in his men.

In 1944, the Chiffrierabteilung was divided into eight groups. Four came directly under Kettler; the other four were combined into two supergroups, Gruppen II and III into Hauptgruppe A for cryptography, Gruppen IV and V into Hauptgruppe B for cryptanalysis, each with its own head who reported to Kettler. This was the organization:

Gruppe Z (Zentralgruppe): personnel; pay, administration; office space and furnishings; Nazi ideological supervision.

Gruppe I: Organization and Control. Referat la: di-

*The term "Nachrichten" reflects this, since it means not only "communications" or "signals" but also "intelligence." In nonmilitary contexts, it means "news" or "information."

rection of the international monitoring service (Chi had intercept posts in Madrid and Seville as well as Lorrach and Tennenlohe, with main posts in Lauf and Treuenbrietzen). Referat Ib: study of foreign communications systems. Referat Ic: provision of teletype communications for Chi and R.S.H.A./VI/MH (former Abwehr).

Gruppe II: Development of German Cipher Methods and Control of Their Use. Referat Ha: camouflage methods for telegraph and radio messages; intercept and wiretapping techniques; cryptographic policy; supervision of cipher employment; cryptographic compromises. Referat lib: development of German cipher systems (camouflage methods, secret writing, secret telephony); supervision of and instruction in cipher production. Referat He: cryptographic systems for radio agents.

Gruppe III: Cipher Supply. Control of production, printing, and distribution of ciphers and keys; operation of the distribution posts (headquarters at Dresden with depots in Halle, Zwickau, Chemnitz, Leipzig, Frankfurt-am-Oder, Bischofswerda, Magdeburg, and Reichenbach).

Gruppe IV: Analytical Cryptanalysis. Referat IVa: testing of suggested German military cryptosystems and telephone scramblers for resistance to crypt-analysis: examination of inventions. Referat IVb: development and construction of cryptanalytic apparatus for Wehrmacht cryptanalytic units; operation of the equipment at Chi. Referat IVc: development of cryptanalytic methods; stripping of superencipherments for Gruppe V. Referat IVd: instruction.

Gruppe V: Practical Cryptanalysis of the Messages of Foreign Governments, Military Attaches, and Secret Agents, Referat V 1-22: national offices. Referat Va: Wehrmacht codewords.

Gruppe VI: Interception of Broadcast and Press Messages. Referat Via: radio reception technique; administration and control of the listening posts at Ludwigsfelde, Husum, Munster, and Gleiwitz. Referat VIb: interception of radioed press and teletype transmissions and of international radio traffic. Referat Vic: surveillance of transmissions from

within Germany to the outside. Referat VId: evaluation of broadcasts and press communication; issuance of the Chi-Nachrichten (a 10- to 20-page daily summary of the non-cryptographic intercepts); special reports.

Gruppe VII: Referat Vila: evaluation and distribution of output. Referat Vllb: chronicles of events (perhaps serving as an information unit).

In addition to these eight sections, a working committee for the testing of German cryptographic security reported directly to Kettler, and half a dozen intercept companies worked for Chi. The office was expected to maintain liaison with the communications units of the Army, Navy, and Air Force; with the chief of army equipment and commander of the replacement army, under whom there was an inspector of signal troops; with the R.S.H.A., the Foreign Office, the Propaganda, Post, Air, Trade, and War Production ministries and, of course, with the party.

(By 1945, the Chiffrierabteilung had been reorganized into seven groups, with functions apparently as follows: Gruppe Z, administration; Gruppe I, organization and control; Gruppe II, Chi-Nachrichten; Gruppe III, broadcast and press interception; Gruppe IV, cryptanalysis; Gruppe V, teletype for Chi and R.S.H.A./VI/Mil; Gruppe X, evaluation, distribution and information services. This downgrading of cryptanalysis and upgrading of the non-cryptanalytic results may reflect a drop in the cryptanalytic results late in the war.)

Chief of Hauptgruppe B, in which the cryptanalytic functions reposed, was Ministerial Counselor Wilhelm Fen-ner, 48 when the war started. A German born and raised in St. Petersburg, he had headed German military cryptanalysis since 1922. He was a brilliant organizer who oversaw the expansion of the group from a handful to more than 150, but he handicapped himself by his egocentricity and by his superciliousness with regard to the noncrypt-analytic aspects of communications intelligence. His right-hand man was a Russian emigrant, Professor Novo-paschenny, who under the Czar had been attached to an astronomical observatory in Pulkovo, outside St. Petersburg. He developed much of the technical aspects of the work, but seems to have held only a relatively subordinate post

as a chief cryptanalyst in one of the national offices, ap parently Referat *V 9,* which was probably Russia.

Head of Analytical Cryptanalysis (Gruppe *TV)* was Dr. Erich Hiittenhain, who also directed that group's instructional activity (Referat IVd). Referat IVa, which tested German cryptosystems, frequently with mathematical tools to calculate theoretical limits of security and to find improvements, was headed by mathematician Dr. Karl Stein, who held the rank of lieutenant, surprisingly low for so lofty a position. Referat IVb, headed by Engineer Wilhelm Rotscheidt, used tabulating machines and special-purpose devices. It invented the prototype of the translucent-sheet-and-light device used by Pers z to strip additives from a known code. The unit first worked out the device for two-digit codes and then extended it to four. Instead of punching out holes corresponding to the most frequent groups, however, Referat IVb marked them with small crosshatched disks, and looked, not for the brightest spot, but for the darkest. Stein's mathematicians extensively investigated the question of how a codegroup stock could be constructed so that this method would not work against it. Referat IVc's chief was Professor Dr. Wolfgang Franz, and Ministerial Counselor Dr. Victor Wendland was head of Gruppe V (Practical Cryptanalysis) and so Fenner's immediate subordinate.

Early in the war, the O.K.W. cryptanalysts worked in a former town house on one of the streets that run off the Tirpitzufer, not far from O.K.W. headquarters on the Bendlerstrasse. About 1943 they moved to much larger quarters in a modern semicircular concrete office building at 56 Potsdamerstrasse called the Haus des Fremden-verkehr—a name that gave rise to many bad jokes because "fremdenverkehr" ("tourist traffic") is German slang for "fornication."

On July 21, 1944, Fellgiebel's sudden removal from command rocked the whole W.N.V. It seemed to be connected with the bomb attempt on Hitler's life of the day before—and it was. Fellgiebel, whose anti-Nazi proclivities had been noted in his fitness report by Keitel, had in fact been a key figure in the plot. He was replaced by Thiele, who became head of both the O.K.W. and the O.K.H. agencies. He served for exactly a month. Then he was arrested as a co-conspirator, his personnel file crossed out with a giant X, and the entry made under his

name, "stricken from the honor roll of the German Army and the Wehrmacht!" Fellgiebel had been executed on August 10; Thiele soon followed. Lieutenant General Albert Praun took Thiele's place in both offices and retained them to the end of the war.

The oldest, most experienced, and closest to O.K.W. of the other cryptanalytic agencies was the Army's Heeres-nachrichtenwesens ("Army Communications System"), or H.N.W. The Chef, H.N.W., served on the Army general staff. Like the U.S. Army's Signal Corps during World •War II, it had both communications and intercept-cryptanalysis duties; like the Signal Corps, it turned over its solutions to Army intelligence for evaluation and use.

Under Chi's watchful eye, it issued cryptosystems for the troops. For high-level communications, from the O.K.H. down to regiments, the Army used the glowlamp Enigma cipher machine. It was reliable, working well in the Russian winter and the Libyan summer. Signal officers thought it cryptanalytically secure if—as ordered by 1942 —keys were changed three times a day. Its chief disadvantage was that it did not print its output. Battery-powered and portable, it could be operated in a moving truck and was well adapted to radio work.

Nevertheless, in 1943 a new machine began replacing it in some areas. This was a printing machine, produced by the Wanderer Werke firm, which copied the Hagelin variable-gear principle. There is a story that one of these was found in Norway at the end of the war with a message still in it, obviously abandoned by an operator who disagreed with what he had deciphered: *Der Fuehrer ist tot. Der Kampf geht welter. Doenitz* ("The Fiihrer is dead. The war goes on, Donitz").

For wire teletypewriter communications from the O.K.H. to army corps and a few divisions, the Germans used an on-line machine produced by Siemens & Halske Aktien-gesellschaft. Its heart was a set of ten keywheels, similar to those on a Hagelin machine, rimmed with pins that could be made either operative or inoperative. Each wheel had a prime number of pins, ranging from 47 on the smallest to 89 on the largest. Five of these wheels enciphered the five teletypewriter pulses, transforming a mark into a space or vice versa if the pin then in position was operative, or leaving the pulse unchanged if it was inoperative. The other five wheels effected a transposition

of the pulses. The machine enciphered and transmitted in a single operation, and likewise deciphered and printed out the message automatically.

Beginning in June, 1942, regiments, battalions, and companies enciphered with the double transposition, with the same keyword for both blocks—the same system, interestingly, as the German Army used at the start of World War I. (This system also backed up the Enigma.) Each division produced at least three keys for its subordinate units. The troops heartily disliked the double transposition, however, and cleartext messages showed a noticeable upsurge. For intelligence and combat reports, these units used small three-letter or three-digit codes, which were likewise published by their divisions. Many cipherers preferred their simplicity to the complexity of the double transposition, and often used them for orders and other unauthorized messages. A signal officer complained bitterly of this practice: "Tarntafeln sind kein Schlusselersatz!" ("Code tables are not cipher substitutes!"), he wrote in a report. Later in the war, a bigrapic substitution replaced the double transposition as a front-line cryptosystem, and in 1944 a modification of the grille replaced that. In addition, the signal troops used numerous special ciphers—for call-signs, numbers, and so on.

The H.N.W. communications-intelligence service operated as a separate organization within an army or an army group, though parts of it were sometimes specially assigned. In 1943, for example, the commander of Fernmeldeaufklarung 7 ("Radio Intelligence 7"), reported to Field Marshal Albert Kesselring. Fernmeldeaufklarung 7 consisted of radio intelligence companies and platoons and direction-finding stations widely scattered over the central Mediterranean area—in western Crete, southern France, northern Africa, Sicily, Sardinia, and Italy. These units reported their intelligence results via their own radio net to the headquarters at Rocca di Papa, south of Rome; the original intercepts were then forwarded to headquarters for more comprehensive evaluation. Fernmeldeaufklarung 7 distributed radio intelligence of tactical importance to the lower commands by broadcasting it in a special cipher. While much of this intelligence came from conversations or radio messages in plaintext or from traffic analysis, much also came from cryptanalysis.

German Army cryptanalysts solved American M-209

messages almost from the days late in 1942 when the two armies first clashed in North Africa. They picked up such tidbits of information as that the 72nd, 45th, and 29th Light and the 71st Heavy Anti-Aircraft Regiments were placed under the 52nd Anti-Aircraft Brigade, which is part of the order-of-battle intelligence basic to a field commander, that on April 1, 1943, the 3rd Infantry Regiment was located at grid square 43835, or 37 kilometers from Gafa, that American forces were forbidden to fire upon airplanes unless the airplanes attacked them (to prevent shooting down Allied planes). All these details were fitted together to give the German command a picture of the troops facing them, their state of mind, their preparation.

Occasionally, a single solved message produced strikingly dramatic results. During a conference at the headquarters of the Commanding General, Southwest, in 1943, Colonel Karl-Albert Miigge, commander of Fernmeldeaufklarung 7, brought Field Marshal Kesselring a British intercept that had just been cryptanalyzed. It reported that in North Africa several troop columns were caught in a traffic jam of their own making by crowding into a wadi at—and here the cryptogram was garbled so that the exact location could not be read. Kesselring called for an immediate air search; the jammed wadi was discovered while the Germans were still in conference. Kesselring promptly ordered an air attack, which wreaked considerable destruction upon the concentrated British forces.

Early in February, 1944, during the Italian campaign, the American 5th Army attempted to recapture the Car-rocetto factory, a pivotal point which the Germans had taken in a counterattack. "It was important for VI Corps not only to regain the Factory area but also to effect the relief of at least a major part of the I Division," the 5th Army historian wrote. "Aided by the 191st Tank Battalion, men of the 1st Battalion made their way into the Factory in the afternoon, only to be driven out. Though our artillery and tanks converted the buildings into a blazing mass of ruins, the enemy held; prisoners reported that an intercepted radio message had given them foreknowledge of the attack. Another attack before dawn on the 12th likewise failed, and the 45th Division gave up the effort to regain the Factory."

As the Allies gained air superiority and the Germans could no longer reconnoiter by air, they depended more

and more on radio intelligence. This was especially true after the Normandy invasion. But this means was not omniscient. In the fall of 1944, when General George Patton's army was preparing to bite out the fortress of Metz, the German forces detected his preparations, largely through radio. "Yet," wrote a German staff officer, "the actual attack on 8 November came as a surprise to the front line troops."

In the field, the German Army's communication intelligence unit worked closely with the Luftwaffe's Funkauf-klarungsdienst ("Radio Reconnaissance Service"). This was the intelligence side of the Air Force's Nachrichten-Verbindungswesen, or N.-V.W. ("Intelligence and Signal System"), whose chief served on the staff of the O.K.L. He also prescribed secret communications systems for the Luftwaffe. Air-to-air communications, which were mostly by voice, employed simple codewords to disguise unit names, much as American pilots referred to one another as EASY RED or GREEN ARROW in the style made familiar by war movies. Air-ground communications were encoded in small three-digit or three-letter codes. Luftwaffe ground-to-ground cryptography used the Enigma.

The Funkaufklarungsdienst employed more than 10,000 men. Its largest subdivision was Luftnachrichten ("Air Intelligence") Regiment 351, with 4,500 men, which intercepted, solved, and evaluated the radio traffic of Allied light and heavy bombers, fighters, transports, and air staffs in Western Europe. An additional unit of 1,000 provided further detailed information on the heavy bombers. Smaller regiments covered other theaters. Luftnachrichten Battalion 350, with 800 men, served as the Luftwaffe center for basic cryptanalysis and traffic analysis, as well as for the study of new enemy radars and radio navigation systems to find the best means of jamming or deceiving them. It also covered the Allied transatlantic air transport service. It was attached to the main headquarters of the Funkaufklarungsdienst.

Other cryptanalysts served in outlying Funkaufklarungsdienst units, solving messages in systems whose basic solution had been worked out at headquarters. They had reportedly tried to use women in teams for solving a widely used Allied air-ground system, called SYKO, but switched to male students when the women did not produce satisfactory results. They tested the youths by crossword puzzles

and sent the 10 per cent doing the best to a training school for about a month. Here they were trained in SYKO cryptanalysis and nothing else. As an incentive, the Nazis told the trainees that the lower 90 per cent of the class would be shipped off to the Russian front.

It was probably not SYKO that enciphered the message that gave the Funkaufklarungsdienst one of its greatest triumphs, since the message originated in a high-echelon ground command and was directed to other ground commands, while the planes themselves maintained radio silence. These were 178 four-engined Liberators, heading for the Rumanian oil fields at Ploesti, Hitler's chief source of oil for his thirsty war machine, in one of the longest-range and potentially one of the most important air strikes of the war. As they lumbered into the air at Bengazi on the morning of August 1, 1943, for their 1,200-mile flight, the 9th Air Force spread a short message to Allied forces in the Mediterranean area announcing that a large mission was airborne from Libya. This was necessary because only a few weeks before, in the invasion of Sicily, the U.S. Navy had shot down dozens of American troop planes in the tragically mistaken belief that they were German bombers.

The message was picked up by a Funkaufklarungsdienst unit recently posted near Athens. Soon its cryptanalysts had reduced it to plaintext. Lieutenant Christian Ochsen-schlager then passed to all defense commands "interested or affected" a message stating that a large formation of four-engined bombers, believed to be Liberators, had been taking off since early morning in the Bengazi area. This gave the antiaircraft defenses at Ploesti, the heaviest in Europe, plenty of time to get ready. When the bombers roared at derrick-top height over the Rumanian oil field, with its wells, refineries, and tanks, they were met with the worst flak encountered by American bombers during the war. Of the 178, 53, or almost every third plane, were downed, and dozens of Americans died.

The German cryptanalytic agency that probably had the greatest effect upon the course of the war was also the smallest and least known. It belonged to the O.K.M., and Grand Admiral Karl Donitz, commander of the German Navy during the latter half of the war, called it his "B-Dienst," for "Beobachtung-Dienst" ("Observation Service"). The B-Dienst had little contact with the other codebreaking agencies. Yet its successes were more far-

reaching than any of theirs, and it participated in some of the most unusual activities of the cryptanalytic war.

Stung in the 1920s by revelations of Room 40's readings of German naval traffic, the O.K.M. built up so effective a cryptanalytic unit that by the start of World War II the B-Dienst had solved some of the most secret Admiralty codes and ciphers. The penetration of British naval messages enabled German surface raiders to elude the British Home Fleet, spared German heavy ships from many a chance encounter with stronger British forces, permitted surprise attacks on British warships, and helped sink six British submarines in the Skagerrak area between June and August of 1940.

Perhaps its greatest feat came in the Norway invasion. On March 1, Hitler approved the plan to invade Norway, but set no date for it. Soon thereafter, the B-Dienst solved British naval messages that revealed a British plan to mine the entrance to Narvik, far in the north of Norway, and to occupy that port; Britain intended to block German ore shipments. This information enabled the German high command to shape a strategy for surmounting the greatest difficulty in its Norway invasion: how to move its weakly guarded transports from Germany to Norway without interference by the powerful British fleet. When the British Narvik expedition was under way, the high command plotted, Germany would send out a decoy force which the British would think was heading to attack their expedition at Narvik. To protect it, Britain would send the rest of its naval forces away to the north. As soon as this happened, the transports would cross the Skagerrak without fear of major sea attack.

The scheme worked to perfection. Late in March the B-Dienst showed British vessels en route to Narvik. On April 2 Hitler set the invasion for the 9th. The decoy force put out to sea and was spotted on the 7th by the British. As the Germans expected, the Admiralty ordered the Home Fleet and the 1st and 2nd Cruiser Squadrons to head for Narvik. As they raced away from where the action was, the German transports completed their voyage undisturbed by the nation that supposedly rules the waves and landed their occupation troops without a hitch. Even Winston Churchill admitted that Germany had "completely outwitted" Britannia.

The B-Dienst may have gained a great deal of help

from some spectacular coups by the German merchant raider *Atlantis.* This specially fitted high-speed freighter, whose heavy armament was carefully camouflaged, was one of several that cruised the oceans and harassed Allied shipping. On July 10, 1940, in one of her first actions, *Atlantis* fired a few shots into *City of Baghdad* in the Indian Ocean and captured the vessel almost intact when her crew hastily abandoned ship. A boarding party reached the officers' cabins just in time to point a pistol at the captain and stop him from throwing overboard most of the ship's secret papers. Among them was the Allied *Merchant Ships' Code,* a two-part code issued by the Admiralty for messages via the Broadcasting for Allied Merchant Ships, or BAMS, commonly called the "BAMS code."

Also recovered were several superencipherment tables, though not the current ones. *Atlantis,* however, had aboard in her special crew a wireless operator named Wesemann who had served for three years in one of the German cryptanalytic services. Wesemann achieved what might be the first nautical cryptanalysis on record when, on the basis of the captured code and several merchant messages that he had intercepted, he succeeded in reconstructing about one third of the superencipherment table then in use. As a result, *Atlantis* could read much of the Allied merchantmen's traffic and could await her victims at likely spots.

When the tables were changed, Wesemann partially reconstructed the new ones with the help of some messages found in the wastebasket of the radio shack of another captured vessel, *Benarty.* The work was completed for him by the B-Dienst, which deduced from his radio queries that he had obtained the BAMS code and consequently sent him the interpretations he needed. Since *Atlantis* and Berlin were then almost at antipodes from one another, this must rank as the longest-distance cryptanalytic collaboration known. A few months later, on November 11, 1940, the crew of the German raider found aboard *Auto-medon,* the 13th ship she had sunk, another copy of the BAMS code and superencipherment tables 7, 8, and 9. All the cryptanalyzed information contributed to *Atlantis'* record as the war's deadliest sea raider.

She may have sent the B-Dienst photographs of the captured codebooks when one of her prize ships returned to

Germany, or the B-Dienst may have obtained a copy elsewhere. Either way, the German knowledge of merchant messages vastly improved U-boat attacks. And, wrote Churchill, "The Battle of the Atlantic was the dominating factor all through the war. Never for one moment could we forget that everything happening elsewhere, on land, at sea, or in the air, depended ultimately upon its outcome." More than once, the B-Dienst placed in the hands of the U-boat commanders the knowledge that brought them to the edge of victory.

In 1941, for example, the B-Dienst read messages to convoys from the Commander in Chief, Western Approaches, that directed those convoys from the danger zones just west of the British Isles. With this intelligence, the U-boat command had no difficulty in deploying its submarines to the maximum effectiveness. Allied losses mounted steeply. In March, April, and May, U-boats sank 142 vessels, or more than one every 16 hours. In January and February of 1943, the B-Dienst mastered British naval cryptosystems so fully that it was even reading the British "U-Boat Situation Report," which was regularly broadcast to the commanders of convoys at sea, telling them the known and presumed locations of U-boats! "These 'Situation Reports' were of the greatest value to us in our efforts to determine how the enemy was able to find out about our U-boat dispositions and with what degree of accuracy he did so," wrote Admiral Donitz.

The following month, March of 1943, saw the climax of the Battle of the Atlantic. And the climactic action, the greatest triumph of the U-boats, in which they very nearly severed Britain's lifeline, stemmed directly from a series of B-Dienst solutions.

The first came on March 9. A B-Dienst report gave the precise location of the eastbound convoy HX 228. (The HX stood for Halifax, Nova Scotia, assembly point for all fast convoys. Slow convoys, which started at Sydney, Cape Breton Island, Nova Scotia, were designated sc.) Shortly thereafter, the B-Dienst reported that the next fast convoy, HX 229, was southeast of Cape Race, steaming on a course of 89 degrees. On the 14th, another solution revealed that a third convoy, sc 122, had received orders at noon the day before that on reaching a given point it was to steer 67 degrees. The U-boats, then operating in wolf packs of two or three dozen, were ordered to search for the convoys.

On the morning of March 16, they sighted a convoy which turned out to be HX 229, and in the next two days, 38 U-boats sent 13 ships to the bottom. Meanwhile, HX 229 overtook the slow-moving sc 122, forming a large mass of shipping in a small space of ocean. The wolf pack nipped at its edges and sank eight more vessels, making a total of 141,000 tons sunk in the three-day battle, at a cost of only a single U-boat. Donitz

exulted: "It was the greatest success that we had so far scored against a convoy."

The Admiralty despaired. They considered abandoning the convoy system as ineffective, which was tantamount to an admission of defeat, since no alternative existed, the loss rate of single vessels being double that of ships in convoy. "The Germans never came so near to disrupting communications between the New World and the Old as in the first twenty days of March, 1943," the naval staff later recorded. It marked the darkest hour of the longest, most crucial battle of the war. And in large measure German cryptanalysts had cast this pall upon Britain by—paradoxically—throwing light upon British communications.

## 13 Duel in the Ether: II

ITALY RELIED for her communication intelligence upon her Army and her Navy. The Navy's cryptanalysts formed the B section of the Servizio Informazione Segreto, or naval intelligence. Early in 1942, they had penetrated the British naval ciphers in the Mediterranean—these were so poor that Admiral Sir Andrew Cunningham reportedly threatened after the invasion of Crete to transmit entirely in clear if he were not given better ciphers. The Italian solution of a British scout plane report enabled the Italian high command to warn one of its task-force commanders at 6 p.m. March 27, just before the Battle of Cape Matapan, that the English had sighted him soon after he had put to sea. Next day the reading of an order to Cunningham from Alexandria made the Italians certain that British torpedo planes would attack. They did, and so prepared were the Italians that the intensity of their antiaircraft de-

fense made it almost impossible for the English to identify their targets or observe the results of the attack.

The Italian Army's security and intelligence organization, the Servizio Informazione Militare, or S.I.M., had a large and well-organized cryptologic section which solved diplomatic as well as military cryptograms. This was its Sezione 5, headed by General Vittorio Gamba, an old Alpine warrior with austere features. A long-time student of cryptology and author of an excellent article on the subject in the *Enciclopedia Italiana,* Gamba was a noted linguist who reputedly knew 25 languages. He came to public attention in 1911 when he translated a series of proclamations into Arabic during the Italo-Turkish conflict over Tripoli. The 50 members of Sezione 5 were housed in a large apartment house in Rome far from S.I.M. headquarters but connected by teletypewriter with it and with the extensive intercept unit, Sezione 6, located on the Forte Bocea, a hill behind the Vatican. Gamba's crypt-analysts maintained close liaison with the chemical section, which worked with secret inks and other means of steg-anography, with the censorship section, and with the phototypographic section, which rapidly reproduced stolen documents.

Like their O.K.W. colleagues, the Sezione 5 cryptanalysts had solved the military ciphers of Yugoslavia, with whom Italy's relations had been strained over Fiume and Trieste practically since Yugoslavia was created after World War I. The Germans used the solutions for a blitzkrieg from the north. The Italians exploited them in a crafty deception that helped avoid a possible debacle in the south.

Almost up to the moment of the Axis invasion, the Italian armies that had occupied Albania had exposed what Churchill picturesquely called their "naked rear" to Yugoslavia in the north. Yugoslavia had no chance against the Wehrmacht, but both Axis and Allies realized that if she struck forcefully against the rather disorganized Italians, she could win a major victory, embarrass Mussolini, delay the Axis conquest, and acquire the munitions and supplies for a large-scale guerrilla harassment of the Nazi occupiers. Thus, when two Yugoslav divisions drove southward on April 7—one from Cetinje toward Shkoder, the other from Kosowska Mitrovica toward Kukes—it was regarded as a serious business. Especially when, by April 12, the Cetinje division had shoved the Italians back to the gates

of Shkoder and was pummeling them with attacks of increasing intensity.

At this juncture the Servizio Informazione Militare got an idea. It drafted two telegrams in Yugoslav military style and affixed the signature of General Dusan Simovic, head of the new government. One read:

> To the Cetinje divisional headquarters:
>
> Subordinate troops will suspend all offensive action and retire in the direction of Podgorica, organizing for defense.

And the other:

> To the Kosowska Mitrovica divisional headquarters:
>
> Withdraw immediately with all subordinate troops back towards Kosowska Mitrovica.
>
> Simovic

Both messages were enciphered in the Yugoslav Army system, and at 10 a.m. on April 13, an S.I.M. station, observing all Yugoslav radio regulations as to wavelength, transmission times, and subordinate stations, contacted the two divisional stations and passed the messages, both of which were receipted for. The drive toward Kukes slackened immediately. The Cetinje division, however, requested confirmation. None came.

Next morning, the confused divisional command, not having received any disavowal of the enciphered orders, and consequently believing that they were valid though incomprehensible lifted its attacks at Shkoder and began retreating northward. The Italians hastened to fill the military vacuum that was created, and marched the 10 miles from Kotor to Cetinje in a day. Next day the Yugoslav headquarters replied that no retreat had been ordered, but by then it was too late. It only told the Yugoslavs that their ciphers were compromised, and, unable to issue new ones in the fluid situation, they attempted to assure the legitimacy of their communications through onerous controls. Instead they gummed their command machinery at a time when every hour counted. A few days later it was all over. The S.I.M.'s fake messages had saved Italy from a crippling defeat.

In a typical month during the war the S.I.M.'s Sezione

6 intercepted 8,000 radiograms. About 6,000 were considered worthy of study, and of these, Sezione 5 reduced 3,500 to plaintext. So great was the flow that General Cesare Ame, head of the S.I.M., began to publish a daily Bulletin I, which summarized the most significant information. Its three copies went to Mussolini, to the chief of the general staff, and to the king, through his aide-de-camp. The S.I.M. distributed other important solutions individually to the proper parties.

Diplomatic traffic naturally went to Count Galeazzo Ciano, the Foreign Minister, whose many mentions of the solutions in his famous diary testify to their importance. According to the diary, Sezione 5 read British, Rumanian, and Turkish traffic. The Italians drank as deeply of the stream of that neutral's messages as the Hungarian group that worked for Hottl was to do. For more than two years, Turkish cryptograms told the Italian government of rumored Allied war plans, of Allied views, of an uncommitted observer's comments on Axis programs and prospects. On January 4, 1943, Ciano jotted in his diary: "The Duce asked me to give [Hans Georg] von Mackensen [German ambassador to Italy] a copy of a telegram the Turkish ambassador Zorlu sent to his government from Kuibyshev. It is a description of the Soviet situation. It seems impartial and quite informative. According to him, the war weighs heavily on the Russians, but Russia is still strong, and, in the judgment of the diplomatic corps in Kuibyshev, Axis stock is falling."

Though Sezione 5 solved many cryptograms, many of its successes came, not from cryptanalysis, but from the S.I.M.'s theft of cryptologic documents. In 1941 alone, the S.I.M. obtained possession of about 50 such items, or about one a week. Some of these probably were only plaintext versions of coded telegrams. But many were the codes or ciphers themselves, and one of them, which led to probably the greatest Axis communications-intelligence results of the war, was a secret code of the United States of America.

The spy who stole it appears to have been Loris Gherardi, a messenger in the office of the American military attaché in Rome. An Italian national just turned 40, he had worked for the Americans since about 1920. His duties included the carrying of telegrams from the attache's office to the Italian telegraph bureau. In August of 1941

he apparently obtained for the S.I.M. the key or an impression of the key or the combination to an embassy safe. This enabled the Italians surreptitiously to open the safe, remove and photograph the BLACK code and its attendant superencipherment tables, and then replace them. Neither his boss, the military attache, Colonel Norman E. Fiske, nor the ambassador ever suspected a thing. Loris continued on the job.*

The BLACK code, so called for the color of its binding, was a relatively new and secret military ATTACHÉ code, with its own superencipherment tables. Ambassadors may also have used it. Thus Ciano gloated in his diary on September 30, 1941, shortly after the theft: "The military intelligence service has come into possession of the American secret code; everything that [U.S. Ambassador William] Phillips telegraphs is read by our decoding offices. . . ."

Soon after the S.I.M. acquired the code, it gave a copy to Germany's Abwehr. From that moment, the Axis powers —subject only to their ability to strip the superencipher-ments—were enabled to peer into the secret messages of the diplomats and the military attaches of a great power that their enemies were seeking desperately to win over. And the messages came from all over the world, not only from Axis capitals, but also from Allied capitals where the American attaches had access to some of the most intimate secrets of the Axis' foes. "I handed Mackensen," Ciano noted on February 12, 1942, "the text of a telegram from the American military ATTACHÉ at Moscow, addressed to Washington. It complains about failure to deliver arms promised by the United States, and says that if the U.S.S.R. is not aided immediately and properly she will have to consider capitulating."

But the most valuable material dealt with the battle-fronts, where the issue of victory or defeat was being decided. In the fall of 1941, the Germans were driving eastward on two fronts, Russia and North Africa, intending to link them up in the Near East, make the Mediterranean an Axis lake, march on to India, and meet the Japanese in

*Gherardi stayed on untfl Italy's declaration of war upon the United States closed the embassy. After the war, he coolly asked for his old job back—and got it! He held it until the secret finally leaked out; then, after several interrogations, he resigned, in August, 1949.

Asia, thereby ruling the world and fulfilling Hitler's dream of out-conquering Alexander the Great.

The American military ATTACHÉ in Cairo had much better opportunities to observe military action than his colleague in Moscow, owing to factors of distance, language, and politics, and he took full advantage of these opportunities to do his job. He was Colonel Bonner Frank Fellers, a West Pointer with a varied peacetime experience, including two years as assistant to General Douglas MacArthur. Fellers had been posted to Cairo in October, 1940. He industriously toured the battlefronts and studied the tactics and problems of desert warfare. He asked questions. He kept his eyes open. The British let him in on some of their secrets, hoping that this would improve American equipment lend-leased to Britain's desert forces, but probably withheld some because of his anti-British predilections. Fellers soaked up this great quantity of information and poured it out to Washington in voluminous and detailed reports.

He discussed the British forces at the front, their duties, capabilities, and effectiveness; he told of reinforcements that were expected and supply ships that had arrived, explained morale problems, analyzed the various tactics that the British had under consideration, even reported on plans for local military operations. He carefully encoded his messages in the BLACK code and radioed them to Washington, usually addressed to MILID WASH (Mzfitary Intelligence Division, Washington). And as his transmissions flashed through the ether, listening Axis radio stations—usually at least two, so that nothing would be missed—took down every word. The intercepts were transmitted by direct wire to cryptanalysts, where they were reduced to plaintext, translated, reenciphered in a German system, and forwarded to General Erwin Rommel, commander of the Afrika Korps. He often had the messages only a few hours after Fellers had sent them.

And what messages they were! They provided Rommel with undoubtedly the broadest and clearest picture of enemy forces and intentions available to any Axis commander throughout the whole war. In the seesaw North African warfare, Rommel had been driven back across the desert by the British under General Claude Auchinleck at the end of 1941, but beginning on January 21, 1942, he rebounded with such vigor that in seventeen days he had

thrown the British back 300 miles. During those days he was getting information like this from the Fellers intercepts:

> January 23: 270 airplanes and a quantity of antiaircraft artillery being withdrawn from North Africa to reinforce British forces in the Far East.
>
> January 25-26: Allied evaluation of the defects of Axis armor and aircraft.
>
> January 29: Complete rundown of British armor, including number in working order, number damaged, number available, and their locations; location and efficiency ratings of armored and motorized units at the front.
>
> February 1: Forthcoming commando operations; efficiency ratings of various British units; report that American M-3 tanks could not be used before mid-February.
>
> February 6: Location and efficiency of the 4th Indian Division and the 1st Armored Division; iteration of British plans to dig in along the Acroma-Bir Hacheim line; recognition of the possibility that Axis forces might reach the Egyptian frontier once the armored divisions had been regrouped.
>
> February 7: British units stabilized along the Ain el Gazala-Bir Hacheim line.

These only highlight the outstanding tesserae of the abundantly detailed mosaic which Rommel had available and which helped him win his epithet, "the Desert Fox." And when in May of 1942 his Panzer divisions rolled forward in his supreme effort to conquer Egypt and punch through Palestine to join the Wehrmacht forces from Russia, the intercepted American messages again brought him information of the highest importance. They first told him that the British were planning to anchor their defense line on Mersa Matruh, a town on the Mediterranean coast about 200 miles west of Alexandria; then, when Auchinleck decided that this position was untenable, the intercepts kept Rommel up to date with the British changes of mind.

But even Rommel could not do much without gasoline for his tanks and troop-carriers, and of this he never had enough. The thorn in his side was Malta. This tough little island, a British bastion lying in the Mediterranean between Sicily and the Axis bases in North Africa, served as the base from which Allied ships, planes, and submarines

wreaked havoc on Axis convoys carrying men and supplies to Rommel. Thus Germany and Italy sought to batter it into submission with air raids night and day, while England sought to strengthen and arm it by driving convoys through to her port of Valletta. When the Axis supply line was flowing freely, Rommel scored one victory after another; when the Allies choked off his supply line and his tanks thirsted for petrol, Rommel's mobility in this highly fluid war of movement was seriously restricted, giving the Allies a considerable advantage.

Hence in June of 1942 the British determined to make a large-scale attempt to relieve Malta. They planned to pass convoys through from the east and from the west simultaneously, thus preventing the Axis from concentrating all its might on either movement. To paralyze Italian surface forces, Britain heavily bombed the Taranto naval base, and to minimize Axis air attacks on the convoys, the British planned to destroy Axis airplanes just before the convoys sailed. This they would accomplish by bombing, by swift strikes of motorized forces on airfields near the front, and by sabotage from commandos parachuted onto other airfields deeper within the German lines. Fellers, who was in close touch with the situation, knew of these plans, and on June 11—the day the eastern half of the convoy sailed from Alexandria—he drafted message No. 11119:

> Nights of June 12th June 13th British sabotage units plan simultaneous sticker bomb attacks against aircraft on 9 Axis airdromes. Plans to reach objectives by parachutes and long range desert patrol.
>
> This method of attack offers tremendous possibility for destruction, risk is slight compared with possible gains. If attacks succeed British should be prepared to make immediate use all R.A.F. [Royal Air Force] to support coordinating attacks by army.
>
> Today British making heavy troop movement from Syria into Lybya.
>
> Fellers

He encoded it and filed it with the Egyptian Telegraph Company in Cairo for radio transmission to MILID WASH. The O.K.W. intercept station at Lauf snatched it from the ether at about 8 a.m. June 12. By 9 a cryptanalyst was

working on it to strip the superencipherment; by 10 it had been decrypted; by 11:30 Rommel had it in plenty of time to warn his airfields. On the night of the 13th, as expected, commandos dropped from the sky and strike forces roared in from the east.

The waiting German and Italian forces massacred them. The carefully planned operation failed almost completely. At the three North African airports of Matruba, El Fetejak, and Barce, not a plane was touched; at the K2 and K3 airfields, the British succeeded only in slightly damaging eight craft, all of them repairable in a few days. At three other airfields (Benina in North Africa and Heraklion and Castelli in Crete), where the warnings were either not received or ignored, the British destroyed a total of 18 planes and burned two hangars.

Next day, airplanes that had been saved from destruction by the timely warning delivered heavy attacks upon the convoy from Alexandria, sinking three destroyers and two merchant ships. A U-boat got a heavy cruiser, and when heavy Italian forces sortied from Taranto, the convoy turned back under this threat and the entire operation failed. "The approach to Malta from the eastward remained sealed, and no convoy again attempted this passage until November," wrote Churchill. "Thus, in spite of our greatest efforts, only two supply ships out of seventeen got through, and the crisis in the island continued." And Rommel's pipeline remained open.

With his gasoline supplies assured, at least temporarily, the Desert Fox swept forward in the onslaught he had begun on the moonlit night of May 26-27. Complementing the strategic intelligence that the Fellers intercepts were providing was the tactical intelligence from his highly efficient Fernmeldeaufklarung Company under Captain Alfred Seebohm. This mobile outfit tuned into every British 8th Army radio station, picked up every scrap of chat, ascertained troop and tank concentrations and movements by direction-finding, learned which units were where by analyzing call-signs, studied British cryptograms, and in general provided Rommel with much of the raw data by which he could sniff out the enemy's intentions and then take counteraction of his own.

During the drive to isolate Tobruk, for instance, the Fernmeldeaufklarung Company overheard a radiotelephone conversation in clear at 10:30 a.m. June 16, 1942, be-

tween the 29th Indian Brigade and the 7th Armored Division. From this it appeared that the garrison of the El Adem box, or strong point, intended to attack the Germans that night. The information was passed to Rommel and his intrepid 90th Light Division, who attacked at once, catching the British so off balance that instead of their pum-meling the Germans, Rommel captured El Adem. This enabled him to surround and isolate Tobruk, which unexpectedly capitulated on the 20th, allowing enormous quantities of stores to fall into German hands and giving the daring Panzer leader his opportunity to strike immediately for Suez. It was aid of this sort that prompted Rommel's intelligence officer to call Seebohm's Fernmel-deaufklarung Company "a very important factor in Rommel's victories." The company could also have independently read the Fellers messages with a furnished copy of the BLACK code to save time in getting the information to Rommel.

On July 10, the swirling desert warfare brought the Afrika Korps staff headquarters directly into the path of a British armored thrust. In a brief, fierce spurt of action, the brilliant Seebohm was killed and most of his unit wiped out or captured. Many of their records fell into British hands. This loss deprived the company's replacements of a great deal of necessary information, and at the same time enabled the British to correct many radio-security mistakes. Rommell thus lost the microscope that scrutinized the enemy lines and presented to him so many bits of information.

At about the same time he lost his telescope. The United States appears to have had some suspicion of the leak earlier in the spring, when two officers came out from Washington to check on Fellers' security measures. They cleared him, and perhaps this lulled their fears until new information reached the Allies. Apparently a prisoner of war told the British of the intercepts, and the British, who had themselves broken the BLACK code and its su-perencipherment, using it to read other traffic, now began to pick up Fellers' messages within an hour after he filed them. After ten days of studying his "long, detailed, and extremely pessimistic" reports, they notified American authorities late in June of the leak and perhaps of Fellers' attitude. Fellers himself was never told of the German solutions, but was recalled to Washington, returning in

July.* Later messages from Cairo still contained some noteworthy observations but no broad view of the situation. And when the new military ATTACHÉ there began using the M-138 strip cipher, which defied all Axis attempts at solution, it cut Rommel off from the strategic intelligence on which he had so long depended.

The loss occurred just as he was crossing the frontier into Egypt and seemed to have the Pyramids and victory almost within his grasp. The British 8th Army fell back to its fortified positions at El Alamein, and on July 2 Auchin-leck jabbed out with the first of a series of counterattacks. Rommel, deprived of his most valuable source of information, could no longer take the expeditious measures for defense and offense that he was previously enabled to. On July 4, he reported that he was going over to the defensive. Meanwhile, Britain succeeded in reinforcing Malta, and attacks from there pinched the Axis pipeline. Rommel clamored in vain for fuel.

At the same time, the 8th Army built up a powerful force in secrecy, and concealed not only the date but the direction of its main thrust. Two divisions arrived with 240 guns and 150 tanks. In the old days, the Afrika Korps would have learned of it from Fellers' messages; this time they never knew the two were there. The British had profited from their capture of the Fernmeldeaufklarung files to institute an improved call-sign procedure, tauten cryptographic discipline forward of divisional headquarters, introduce radiotelephone codes, impose rigid wireless silence or reserve formations, pad out real messages with dummy traffic, and create an entire fake signals network in the southern sector. The new Fernmeldeaufklarung staff had neither the talent nor the experience to penetrate these disguises and sift the true from the false. The Germans, who had been used to the constant flow of information from Seebohm's men, had to depend almost exclusively upon ah" reconnaissance, without any radio-intelligence corrective. And camouflage fooled it Hundreds of tanks and guns were hidden beneath dummy trucks; large supply

*Later in 1942 he was awarded the Distinguished Service Medal for his work as military attach^, which "contributed materially to the tactical and technical development of our Armed Forces." The citation also stated that "His reports to the War Department were models of clarity and accuracy."

depots were created so slowly in the south that it looked as if they could not be ready for several months.

So when General Bernard Montgomery opened fire with a thousand cannon on the German positions at Alamein on October 23, it came as a complete surprise to the Afrika Korps. Rommel had been so certain that nothing would happen for a while that he had gone to Austria to convalesce. He flew back at once to take personal charge of the battle, but by the time he arrived it had already been lost. Hampered by shortages of oil, men, and armor, he could only shift his divisions about in desperate but futile attempts to recover. The defeat became a rout, and the Afrika Korps fled west across the desert, leaving a battlefield littered with hundreds of destroyed or useless tanks and troop-carriers. A few months later the Germans were driven out of Africa, then out of Crete, then up the boot of Italy—always retreating, never again advancing. The Battle of Alamein marked the turning of the Allied hinge of fate. "Before Alamein we never had a victory," Churchill said. "After Alamein we never had a defeat."

That change in fortune had revolved, to no small degree, upon cryptology.

Almost certainly the best of the nonbelligerent cryptanalysts, and perhaps one of the best in the war, was that of the precarious neutral, Sweden. At first she used code-breaking primarily to see whether Hitler planned to grant her the same sort of military protection that he so generously accorded Norway and Denmark. His preparation for occupying those two countries was one of the best-kept secrets of the war, and Sweden did not want to be caught napping. Later she used the intelligence to keep abreast of a variety of political events.

Except for a brief interlude back about the turn of the century, when R. Torpadie so impressed the Swedish authorities by solving a nomenclator of 1632 for a historical study that they commissioned him to set up a cryptologic bureau called Room 100, Swedish cryptology got its real start with Yves Gylden. His father, Olof, the head of the Royal Naval School, had been financially interested in Arvid Damm's cipher machines. Yves, who got his un-Swedish first name from his French mother, became cryptologically interested and subjected them to every possible cryptanalytic test The interest thus kindled

in cryptology remained with him throughout a business career with the pharmaceutical firm of Astra, founded by his grandfather. In 1931, a tall, grave man of 36, Gylden published his *Chifferbyrdernas insatser i vdrldskriget till lands,* a keen, perceptive study of World War I cryptology and its effects. Its 139 pages were later translated into English by the U.S. Army Signal Corps as *The Contributions of the Cryptographic Bureaus in the World War,* and portions were published in the *Revue Militaire Fran-false.* This book demolished the lingering myth of chamber analysis, demonstrated the crucial role of errors and of torrents of ciphertext, and generally crystallized the lessons of World War I and catalyzed the evolution of the cryptology of today.

Five years after the influential little book was published, Sweden set up a cryptologic bureau. It was headed by Colonel C. G. Warburg, a gentleman who had fallen off a horse, broken both arms and legs, and needed a sinecure. He proved as incompetent in cryptology as in equitation, and was replaced by a naval officer who won the respect of the experts who later served under him. During the late 1930s Gylde'n gave many talks on cryptanalysis to Swedes. He also sowed the seeds of a valuable cooperation With the other Scandinavian countries when he lectured in Oslo and stimulated Captain Roscher-Lund to set up Norway's first cryptologic office. In 1939, during a 12-hour war game, Gylden headed the cryptanalytical office that solved 38 of the 56 rather simple cryptograms transmitted by the "invaders." Sweden's preparations extended to recruiting talks at Uppsala University, where coeds were entertained with the intrigues of cryptology and sold on the idea that they could become good codebreakers. Other personnel were drawn from the winners of cipher-solving contests which the cryptanalysts got the newspapers to run.

When war broke out, the Swedish cryptanalysts numbered 22. All were paid the magnificent sum of half a crown a day (raised later by stages to two crowns), as a result of which most of them engaged in a kind of part-time cryptanalysis—working for the government in the morning and at regular jobs to get money to live on in the afternoon. They were installed first in the Gray House, Sweden's Defense Ministry building, and afterwards in an old house at Carlaplan 4, since demolished and replaced

by Sveriges Radio; they finally settled down in an old, drafty, noncentrally-heated apartment house at Styrmans-gatan 2. (A branch was also established in a modern apartment house in Strandvagen in 1943.)

In 1940 the cryptanalysts were divided by language, though some of the mathematicians shifted from group to group. The four units were: No. 1, for Romance languages, primarily French and Italian, headed by Gylden, who had spent ten years in France and was fluent in that language; No. 2, for German, in which one of the brightest workers was Carl-Otto Segerdahl, a young mathematician; No. 3, for English, which attacked American and British systems and was headed by Dr. Olof von Feilitzen, 32, a librarian whose English is better than that of many Americans; No. 4, for Russian, headed by Dr. Arne Beurling, 35, a big, slow-talking, quietly handsome professor of mathematics at Uppsala University, who in 1952 became a member of the Institute for Advanced Study at Princeton. Beurling, one of the war's finest crypt-analysts, also determined the unknown ciphers of other countries and made the initial breaks. Gylden, as the founder, was a kind of first among equals; he also taught new recruits. These came in at such a pace that by the time he left in 1941 the group had grown to 500, and by the end of the war to 1,000.

Messages, too, poured in. Teletypewriters, cut directly into Swedish postoffice circuits, duplicated messages sent over those wires. Norway, Denmark, and Finland forwarded their intercepts to Sweden, which had perhaps the best cryptanalytic center among them, and these messages enabled Sweden to make very fruitful comparisons between the same text enciphered in different keys. She paid her Nordic associates back with the information gained in the resultant cryptanalysis—sometimes with valuable results.

Early in 1940, just before the German occupation of Norway, Nazi agents there, who were concentrated in the German-Norwegian shipping lines and in the large fishing and fish-processing firms, were ordered to pass back information on ship movements and weather. They disguised the data as sales prices, offers, and tonnage reports on fishing, and transmitted by telephone and radio. But the Norwegian authorities had intercepted the telephone calls, which dealt with prices in a highly suspicious manner.

They sent recordings to Sweden, where Segerdahl discovered that the five-digit "prices" actually represented the transposed and monoalphabetically enciphered numbers of ships in *Lloyd's Register.* The solutions enabled Norway to break up at least one of the rings in February, though others continued to operate.

The Swedes not only used cryptology against foreign espionage, they sometimes used espionage against foreign cryptology. In one case, they tapped a telephone call between the Italian military ATTACHÉ in Stockholm and his colleague in Oslo. The recording sounded absolutely unintelligible, and the Swedes at first thought that the Italians had used a telephone scrambler. When they determined that they had not, the recording was sent to the language department at Uppsala, where it was found to be a Sicilian dialect rendered incomprehensible by the attache's over-liberal use of cursewords. Eventually the sense was sorted out, and the conversation proved to comprise the Stockholm attache's explanations of how to use the military ATTACHÉ code, which the Oslo man—who was railing at the idiots in Rome who would send him such a code—could not fathom. Between the explosions of the colorful Sicilian equivalents for "dunce" and "jackass" and still other expletives were references to operating procedure, meanings of specific codewords, and so on. Needless to say, it proved a great help to Gylden in his Italian-code solutions.

The Swedes also obtained much help from their own Foreign Office in the form of diplomatic notes sent and received, reports of notes verbales, aides-memoires of conversations with various ambassadors, and other memoranda. This is common practice in all countries, but the Swedish cryptanalysts carried it to a peak of perfection by using as their liaison man a former foreign minister. Rickard Sandier, 56, had served in that post from 1932 to 1939; he had also filled in as premier for 18 months in 1925 and 1926, and in 1934 had been elected president of the League of Nations Assembly. Spare and round-faced, Sandier had been bitten by the cryptology bug, and in 1943 he wrote a book on famous ciphers. But he proved inept as a crypt-analyst, unable to solve what the Swedes regarded as the simplest of practical problems—Norwegian one-part codes. However, he was a great success in making sure that the Foreign Office reported every scrap of information promptly to the cryptanalysts. So well did he have his contacts

trained that the Foreign Office even reported the time of departure of an ambassador's car from the Foreign Office building. With this little datum, the cryptanalysts—knowing the message he had been given and estimating how long it would take the ambassador to drive to the embassy and have a message of that length encoded and sent to the telegraph office—could more easily pick out the cryptogram corresponding to that message from the embassy's daily file.

As usual, the Swedish cryptanalysts were greatly helped by lazy or stupid encoders. Clerks repeatedly violated the most elementary rules by failing to superencipher and forgetting to bisect messages. The worst bungler the Swedes came across was the German consul at Stavanger, whose numerous blunders became the vulnerable heel of many a German message. His name—almost too fittingly—was F. W. Achilles. The Swedes appreciated his help so much that they hung a large photograph of him in their office. "He was very fat and he looked like a gorilla," Segerdahl said. "I never met the man personally, but I considered him my best friend in the German diplomatic service!"

The Swedes also read messages in other German systems —a double transposition for the military ATTACHÉ and two substitution systems for the troops. The latter gave them an unexpected peek into the sex habits of German soldiers. The Wehrmacht provided women from the Baltic states and concentration camps as prostitutes for the occupation forces in Norway, and the vessels were naturally awaited with great eagerness. Their arrivals and departures formed the subject of excited communication between units, and not infrequently a radioman in a port from which a ship had just sailed would recommend one of the girls to a fellow signalman in the port to which the ship was headed. The reasons were sometimes quite specific, and the Swedes came to think that they knew the girls almost as well by cryptologic means as the soldiers did by carnal.

But errors, circular messages, and all the other aids would not have helped the Swedes much if they were not as clever as they were. They became so attuned to French procedure in regard to a multiplicity of codes—at one time the French had eleven in simultaneous use—that they could tell when the French regarded them as compromised (after about four years) and began sending material in them that they wanted others to read. Usually this tried to implant

the idea that the French were acting only out of the most moral considerations in a given situation, probably to distract attention from their real motives. Many phrases from the messages in these compromised codes later showed up in the French Yellow Books, the official governmental statements of their positions. The Swedes also solved an American-British code in which U-boat warnings were transmitted—probably the same that Germany's B-Dienst read—and thus got a free ride in safeguarding their own merchantmen.

Quiet possibly the finest feat of cryptanalysis performed by the Swedes, and the most far-reaching, was Arne Beurl-ing's solution of the German Siemens machine. Since German messages passed over Swedish wires just as German soldiers passed over Swedish rails, both the Wehrmacht in Norway and the German embassy in Stockholm took advantage of the machine's on-line capabilities to wire messages directly to Berlin. The German Foreign Office called the machine the Geheimschreiber ("secret writer"). The teleprinters in the Swedish cryptanalytic bureau rapped out the German correspondence, and it was given to Beurling for an attempt at solution.

He observed at once that the ciphertext consisted of the 26 letters and six digits, a total of 32 characters, or $2^5$. This suggested a cipher based on a teletypewriter to him, since he knew that teletypewriters used a five-hole punched tape. That was about all he knew, though, and he had to get a book on them to see how they worked. His studies— perhaps aided by an examination of patents—led him to the conclusion that a machine based on the Baudot code would encipher by shifting the positions of the five contacts, that each of these positions would very likely be controlled by a keywheel of its own, and that the number of control pins on the circumference of these wheels would vary from wheel to wheel to make the period as long as possible.

Since the key probably changed daily, Beurling selected the traffic for a single day, May 25, 1940, to work on. It covered the equivalent of two large sheets of paper. His analysis soon showed that his preliminary suppositions were correct, except that the substitution of the Baudot pulses was followed by a transposition. Very often the transposition had no effect. If, for example, pulses 1 and 2 were the same, the transposition of 1, 2, 3, 4, 5 into 2,

*i, j, t,* 3 would leave the character unchanged. Beurling took full advantage of these peculiarities to reconstruct the mechanism. He checked his work with new data from the traffic of May 27, found it was correct, and within two weeks of undertaking the job had solved the cipher. A Swedish mechanic constructed an apparatus to Beurling's specifications, and though it looked monstrous and made a terrific racket, it printed out the German messages that the Swedes wanted to read.

To recover the daily keys, the cryptanalysts would work through the night, and in the morning, when the Swedish commander, Lieutenant General Olov Thornell, came in to ask, "What's the news from the Germans today?" they were usually able to tell him. Twice when the Germans made threatening moves with their troops in Norway toward Sweden, Swedish troops, alerted by crypt-analyzed messages, moved swiftly into position and blocked the Germans. Their commander, General Niklaus von Falkenhorst, later extended congratulations to Thornell on the brilliance of his tactics. Thornell passed the felicitations on to the cryptanalysts.

In the spring of 1941, the Swedes cryptanalyzed other German military messages that, put together, spelled an invasion of Russia between June 20 and 25. Erik Bohem-ann, secretary general of the Swedish Foreign Office, passed the information to Sir Stafford Cripps, British ambassador to the Soviet Union, at a dinner in Stockholm while Cripps was passing through. This may not have come as news to Cripps, who may have known of the invasion from other sources, but it certainly reinforced any knowledge he had. Unfortunately, Stalin did not believe the British.

The dozens of diplomatic messages that clattered out of the Beurling mechanism told the Swedish Foreign Office what the Germans were really doing and thinking. They gave Foreign Minister Christian Giinther advance warning of diplomatic notes that the German embassy was ordered to submit to him. The cryptanalysts tell a story that, after reading a particularly demanding note, they took the unusual step of notifying Giinther of its contents by telephone, which they rarely used. (Later they sent it over by the regular messenger, who wore two shoulder holsters.) Giinther promptly went on a "hunting trip," and the German diplomat could not serve his demand until after the weekend. By then the Swedes had formulated a policy that

enabled them to tell the Germans, with suitable regret, that they were unable to fulfill the requests.

And so Sweden's cryptanalysts helped her navigate the perilous waters of neutrality while all about her raged the war.

Great Britain's main cryptanalytic agency lay within her Foreign Office, which had taken over the personnel of the Admirality's Room 40 at the end of World War I. The Reverend William Montgomery, one of the solvers of the Zimmermann telegram, for example, joined the Foreign Office. Early in the 1920s, in a circular urging its diplomats to be more careful in the use of their codes, the Foreign Office told them that it was spending £12,000 a year, or almost $60,000, both in keeping British codes secret and in solving those of foreign governments, and that carelessness in handling codes was wasting much of this (or at least much of the part spent for British cryptography). The usual legends circulated among the diplomats about their code experts, some of whom had "made a life-long study of the work." One story credited one of these wizards with solving a Turkish code during the war in less than five months, though he himself could not speak Turkish and had had to call in experts in the language to translate the messages. The Foreign Office reportedly considered no code as fully secret after it had been used for six months; consequently it changed all highly confidential codes every four months.

In 1939, the Foreign Office moved what it euphemistically called its Department of Communications to Bletchley Park, an estate and mansion in Bletchley, a town in Buckinghamshire about 50 miles northwest of London. It is far and away the most history-redolent black chamber of all. The British, of course, trace the land from a Roman encampment, through its award by William the Con-querer to Bishop Geoffrey of Constance for services rendered at the Battle of Hastings, down on through the ownership of various lords (most notably the two George Villierses, first and second dukes of Buckingham) and rich men of decreasing interest. A mansion was first built on the land in the 1870s and added to repeatedly; the Foreign Office, finding this too small, added many buildings, including a cafeteria and a large hall. Eventually 7,000

wonced and trained there, including members of the armed services.

[Codebreakers 264.jpg]

*Britain urges cryptographic discipline*

The War Office expanded its M.I. 1 (b), the cryptanalytic agency started in World War I in the War Office, to M.I. 8—the same name, coincidentally, as that held by Yardley's organization. The Admiralty and the Air Ministry presumably had cryptologic agencies of their own. One of the first victories of the Admiralty's unit was, surprisingly, in the domain of cryptography.

Since the beginning of the war, Admiralty secret com-munciations had been read by the B-Dienst, with such disastrous results as the loss of Norway almost by default. The Germans continued to listen in to Admiralty messages during the critical summer of 1940 as Hitler prepared for Operation SEALION—his invasion of England. The crypt-analytic intelligence had long been entering into operational planning, and the Oberkommando der Kriegsmarine had come to depend on it. Suddenly, on August 20, as all England was bracing itself in its finest hour, and the sky above was streaked with contrails as the few earned their tribute from the many, the Admiralty, which had finally tumbled to the German cryptanalysis, changed its codes and ciphers. O.K.M. went deaf. The abrupt cutting off of quantities of information about British plans and disposi-

tions caused, a German said, "a great setback for German naval strategy." No longer could German vessels strike out at the greater British forces with foreknowledge or move deftly out of their way. British sea power rapidly gained its normal ascendancy. English ships shelled the invasion fleet in Channel ports. Air reconnaissance alone could not tell the Germans enough. The O.K.M., never very warm for SEALION, chilled still further. Eventually its coolness spread throughout O.R.W., and then to Hitler. It contributed to his ultimate decision to postpone SEALION indefinitely, and hence forever.

[Codebreakers 265.jpg]

*A British naval officer demonstrates the proper codebook security for when capture threatens*

All of Britain's cryptologic work seems to have been coordinated by the Foreign Office's Department of Com munications, which apparently handled strategic and primary cryptosystem solutions. All over the world, Britain had about 30,000 persons in communications intelligence. Deputy director of the Department of Communications was a man who had already made a mark in the world by his cryptanalytic efforts. He was Nigel de Grey, who in 1917 had solved the Zimmermann telegram.

The department turned out solutions at a fairly rapid

I

rate. On November 21, 1941, a Japanese diplomatic solution was given number 097975; on December 12, another Japanese diplomatic solution was numbered 098846;— indicating almost 300 solutions a week at that time (not Japanese alone, of course). A typical distribution of these solutions would send three copies each to the director of the department, the Foreign Office, and the War Office, two to the India Office, and one each to the Admiralty, the Air Ministry, the Colonial Office, the Dominion Office, M.I. 5 (counterintelligence), and Sir Edward Bridges, secretary to the Cabinet. The appearance of Bridges' name on the list suggests that some of the British intercepts may have been read aloud at Cabinet meetings. In addition, Churchill, on August 5, 1940, ordered that a daily selection of original intelligence documents be submitted to him personally "in their original form," which almost certainly included intercepts. Much of the cryptanalytic output must have gone to the Joint Intelligence Committee, which evaluated all intelligence. It was always chaired by a Foreign Office representative, who was Victor F. W. Caven-dish-Bentick throughout most of the war, and included the directors of military, naval, and air intelligence.

The intelligence from these solutions went also to the United States, but so closely did Britain guard her crypt-analytic capabilities that for more than a year she would give the United States information based on the crypt-analyses but would not name the source. In January, 1941, however, a four-man American cryptanalytic mission accompanied a PURPLE machine to England to establish technical cooperation with British cryptanalysts. Britain had not cracked the PURPLE machine, but they had more in the way of cryptanalyzed intercepts than the United States, and this was the quid pro quo. This cooperation between the two English-speaking nations in the most sensitive of areas tells the depths of their friendship. The American Signal Intelligence Service and OP-20-G radioed the PURPLE keys to London daily. Cooperation extended to the small Australian communications-intelligence unit and to the unit at Singapore, and Canada assisted in making sure that all got all Japanese intercepts.

Among the characteristic features of World War II was the extensive use of codenames to designate important operations or secret projects. Codenames had been used

before—the words "tank" and "blimp" themselves derive from World War I codenames—but never so frequently. They aimed both at security and brevity: obviously it was easier to say "Operation TORCH" than "the Anglo-American invasion of North Africa," and solvers of any messages would still have to determine the meaning of the code-names.

Selection and assignment of the codenames was, in the United States, a duty of the Current Section of the Army's Operations Division. Men of the unit culled the unabridged dictionaries for suitable words—chiefly common nouns and adjectives that did not imply operations or localities. They avoided, as confusing, personal and ships' names and geographical terms. Of the dictionaries' 400,000 words, they compiled about 10,000 in scrambled order in a classified book. They cross-checked these to eliminate any conflicts with British codenames. Then they assigned blocks of codenames to theater commanders.

In theory the codenames bore no relation, either by denotation or connotation, to what they stood for. In the majority of cases this held in practice. FLINTLOCK meant the Allied attack on the Marshall Islands in 1944; AVALANCHE, the amphibious attack on Salerno; ANVIL, later DRAGOON, the Anglo-American landings in the soft underbelly of France. Even relatively small operations were dubbed: the relief of Australians trapped in Tobruk was SUPERCHARGE, the occupation of the Canary Islands was PILGRIM. Some codenames were written in blood: OMAHA, UTAH, GOLD, SWORD, and JUNO, for the Normandy beaches of D-Day.

The allied codename selections were sometimes constrained by principles that that master of English, Winston Churchill laid down in a memorandum of August 8, 1943:

> I have crossed out on the attached paper many unsuitable names. Operations in which large numbers of men may lose their lives ought not to be described by code-words which imply a boastful and overconfident sentiment, such as "Triumphant," or, conversely, which are calculated to invest the plan with an air of despondency, such as "Woebetide," "Massacre," "Jumble," "Trouble," "Fidget," "Flimsy," "Pathetic," and "Jaundice." They ought not to be names of a frivolous character, such as "Bunnyhug," "Billings-

gate," "Aperitif," and "Ballyhoo." They should not be ordinary words often used in other connections, such as "Flood," "Smooth," "Sudden," "Supreme," "Fullforce," and "Fullspeed." Names of living people —Ministers or Commanders—should be avoided, e.g., "Bracken."

2. After all, the world is wide, and intelligent thought will readily supply an unlimited number of wel-sounding names which do not suggest the character of the operation or disparage it in any way and do not enable some widow or mother to say that her son was killed in an operation called "Bunnyhug" or "Ballyhoo."

3. Proper names are good in this field. The heroes of antiquity, figures from Greek and Roman mythology, the constellations and stars, famous racehorses, names of British and American war heroes, could be used, provided they fall within the rules above. There are no doubt many other themes that could be suggested.

4. Care should be taken in all this process. An efficient and a successful administration manifests itself equally in small as in great matters.

The Americans demonstrated a like sensitivity when they codenamed the crowning operations of the Pacific War, the invasion of Japan, CORONET and OLYMPIC. But it remained for Churchillian eloquence to find the great codename of the war for the greatest operation of the war. The name evoked a sense of majesty and patriarchal vengeance and irresistible power for the supreme Allied effort to enter the continent of Europe and crush forever the wicked Nazi conspiracy. The master wordsmith himself consecrated that crusade with the codename Operation OVERLORD.

Before that vast offensive could be mounted, the Allies had to win the Battle of the Atlantic. In this, communications intelligence played a role of high importance. Indeed, in some respects the Battle of the Atlantic might be viewed as a duel between the Axis and the Allied cryptanalytic organizations. And while Donitz' B-Dienst had its successes, the Allied communications intelligence

agencies enjoyed the advantage of access to the extremely heavy traffic of the U-boat fleet.

In part, this stemmed from Donitz' insistence on maintaining tactical control of his submarines so as to concentrate them in wolf packs on the richest prizes. He was aware of the danger in all the talk, but, he contended, "The signals from the U-boats contained the information upon which was based the planning and control of those combined attacks which alone held the promise of really great success against the concentrated shipping of any enemy convoy." His encouragement of communication led to an almost complete relaxation of radio discipline. U-boats went on the air to report a toothache on board or to congratulate a friend at headquarters on a birthday. U-boat command became "the most gabby military organization in all the history of war."

Thanks to Commander Laurance F. Safford, head of OP-20-G and father of the Navy's communications-intelligence organization, the United States had, upon its entrance into the war, an Atlantic arc of high-frequency direction-finders to exploit the U-boat garrulity. Stations reported their bearings to their net control center in Maryland, whence they were flashed to the naval communications-intelligence organization at 3801 Nebraska Avenue, North West, in Washington. Commander Knight McMahon and his staff combined them into fixes and flashed these to the Atlantic Section of the Navy Commander in Chief's Combat Intelligence Division. From here they sped to antisubmarine forces.

How fast this net—called "huffduff' from the HF/DF abbreviation of "high-frequency direction-finding"—could work was shown by the episode of June 30, 1942. That morning, *U-158* went on the air to report to Donitz that he had nothing to report. Huffduff stations at Bermuda, Hartland Point, Kingston, and Georgetown heard him. McMahon plotted his positiori as latitude 33 degrees north, longitude 67 degrees 30 minutes west. This information raced down through channels until it reached Lieutenant Richard E. Schreder, U.S.N., flying an antisubmarine patrol out of Bermuda. Ten miles from the spotted location he found *U-158* loafing on the surface, its crew sunbathing. One of Schreder's depth charges landed on the submarine's superstructure just as it was trying to dive. It went down all right, but it never came up.

In another case, huffduff hounded a U-boat to death. The net first heard a transmission of *U-66* on April 19, 1944, and followed her successive messages in her attempts to rendezvous with a supply submarine. Allied ships, told where to go by huffduff, repeatedly frustrated these efforts, and on May 5 her commander wirelessed home: "Refueling impossible under constant stalking. Mid-Atlantic worse than Bay of Biscay." Her "spurt" transmission—made by tape-recording the message and then radioing the tape at high speed—lasted less than 15 seconds, but no fewer than 26 huffduff stations got bearings on it, probably as a result of improved equipment that scanned the horizon 20 times a second and zeroed in accurately and semiautomatically on any emission. Three hours later, an American plane spotted the U-boat; an hour after that an American ship began to attack it, and within 25 minutes the submarine had gone down.

In addition to huffduff, an intercept network eavesdropped on the text of the German messages. The Navy monitors could often tell one U-boat from another by the sending characteristics of their radio operators, and sometimes could ascertain the number of U-boats in a wolf pack. They grew so familiar with the submarine signals that they sometimes knew simply from external characteristics that a given message was a convoy contact report or a signal that attack had begun.

Help was obtained from the most exciting code theft of World War II. It took place on the high seas with lightninglike speed under conditions of great peril.

Early in 1944, Captain Daniel V. Gallery, U.S.N., commanding the antisubmarine Task Group 22.3, conceived a daring plan for boarding a U-boat and capturing it if, as sometimes happened, it surfaced after depth-charge damage to allow its crew to escape. Even though the plan as a whole might fail, he might pirate the submarine's cryptographic equipment, which alone would make such a venture worthwhile. So he trained a team of volunteers in dismantling booby traps, closing sea cocks, and handling a U-boat.

On May 31, 1944, be began tracking *U-505,* which huffduff had discovered was apparently heading for its home port at Brest. At 11 a.m. Sunday, June 4, a clear day with a light breeze, he made sound contact with the U-boat about 150 miles west of Cape Blanco, French West Africa. Its captain was at lunch when a salvo of depth

charges slammed the peacefully gliding vessel, holing the outer hull and convincing him that his ship was mortally stricken. He blew his tanks and surfaced, and as his crew boiled out of hatches and the conning tower and leaped into the sea, U.S.S. *Pillsbury* was lowering a whaleboat carrying the boarding party.

A few moments later, it reached the abandoned sub, rocking gently in the long Atlantic swells. Lieutenant (j.g.) Albert L. David, leading the boarding party, and petty officers Arthur K. Knispel and Stanley E. Wdowiak slipped through the hatch, raced forward to the radio room, smashed open a couple of lockers, and grabbed the cryptographic equipment—the current codebook with superenci-pherments, the Enigma machine and its list of keys, and hundreds of messages with parallel plaintexts and cipher-texts. The Germans had apparently never considered the possibility of a boarding and so had not bothered to jettison the material. The three Americans hastily passed the items up on deck so that the team would have something to show for its efforts even if it lost the sub.

But within fifteen minutes, the team had disconnected demolition charges and shut off an eight-inch stream of water, and *U-505* had become the first enemy warship captured by a U.S. Navy boarding party since the War of 1812.

The Allies now read U-boat operational traffic. For they had, more than a year before the theft, succeeded in solving the difficult U-boat systems and—in one of the finest cryptanalytic achievements of the war—managed to read the intercepts on a current basis. For this, the cryptanalysts needed the help of a mass of machinery that filled two buildings.

What all this did to the submarines was graphically described by the German naval officer Harald Busch: "In the latter half of 1944 no U-boat commander would incur the ordeal of refueling if he could possibly avoid it. ... on a suspiciously large number of occasions, enemy aircraft had made their appearance at the very moment when the pipeline was stretched between the two boats and neither was able to dive, with the result that many U-boats had been destroyed in the act of refueling. . . . Evidently U-boat commanders were right in their suspicions: the enemy could and did decipher the signals transmitted by Admiral Donitz' headquarters in Berlin."

in the eleven months remaining before the end of the European war, the Allies, greatly aided by the information that told them where to send their now powerful air and naval forces, sank nearly 300 U-boats—almost one a day —and greatly reduced their shipping losses. "Battles might be won or lost," Churchill wrote, "enterprises might succeed or miscarry, territories might be gained or quitted, but dominating all our power to carry on the war, or even keep ourselves alive, lay our mastery of the ocean routes and the free approach and entry to our ports." These the Allies mastered. "Reduced to the simplest terms," wrote one author in a study of the Battle of the Atlantic, "the Allies won the U-boat war and Germany lost it because Donitz talked too much."

Final victory over the Nazi evil could come only by driving a military stake through its heart, and in this mission communications intelligence played an important role. The march actually began in North Africa in 1942 under the pressure for a "Second Front Now." Communications-intelligence units were there—though not exactly in the role assigned them. Radio-intelligence companies of the American Army charged ashore as assault troops! They soon resumed their proper duties, however, and, equipped with intercept receivers and direction-finders, began to eavesdrop on the Axis messages. During the Tunisia campaign, the 128th, 117th, 122nd, 123rd, and 849th Signal Companies (Radio Intelligence) tracked the Germans all over North Africa and, by monitoring American communications, plugged leaks in Allied radio security. The 128th first discovered that the Germans were withdrawing from the Kasserine Pass, which they had taken a few days earlier in America's first blooding *in* Europe. Later the 128th gave advance warning of several enemy attacks. In Italy, the VI Corps intelligence officer said that his radio intelligence platoon had done "outstanding" work during the march on Rome and had supplied information second in value only to battle reconnaissance. Thus, even though the manning and equipping of radio intelligence companies did not get under way until relatively late in the war, officers in the field soon declared their product to be "of material value ... at times vital" and praised the units as among the "most constantly profitable sources" of intelligence on German plans and movements.

Strategic communications intelligence about German in-

tentions in the European war mainly came, however, from Japanese sources. This should not be surprising. The Wehrmacht had the advantage of interior communications throughout occupied Europe and so could use wire networks, which offer very little opportunity for interception. But the Japanese diplomats in Berlin, Rome, Madrid, Lisbon, Sofia, Budapest, and Moscow had no way of getting messages back to Tokyo but by radio. These the Allies intercepted.

The messages of the Japanese military attaches, whose code the United States had broken, yielded quantities of information. This source was lost to the Allies in 1943 in an ironic development that demonstrates the superiority of cryptanalysis over theft as a secret source of information. The Office of Strategic Services, America's new spy outfit, in a laudable attempt at espionage, penetrated the offices of the Japanese embassy in Portugal. They did not disclose their plans to the Army, whose Signal Security Agency (formerly the Signal Intelligence Service) had broken the code; nor did the Army warn the O.S.S. against doing anything that would jeopardize its cryptanalyses. The upshot was that the Japanese discovered traces of the search, decided that their military ATTACHÉ code might have been compromised, and changed it. The Allies, who had been comfortably reading the messages without benefit of espionage, still had not broken into the new code by the fall of 1944. Thus the attempt to gain information by cloak-and-dagger methods deprived the United States of information that it had been obtaining by the traceless means of communications intelligence.

Bulky cipher machines such as the Japanese diplomats used could not be shipped or smuggled into blockaded Europe very easily, and so PURPLE remained in service throughout the war. Quite probably the Japanese considered the system secure. But even before Pearl Harbor American cryptanalysts were reading Japanese PURPLE messages from Berlin, and they preyed upon them even more avidly after the United States entered the war. Thus William F. Friedman's solution of PURPLE reverberated throughout the war, leading to major effects and making it one of the world's great cryptanalyses not only in technique but in importance as well.

The Germans granted the Japanese ambassador, Baron Hiroshi Oshima, the intimacies of an ally, and, as a former

military attache, he took considerable interest in the military sphere. Toward the end of October, 1943, when it became evident that the Allies would invade Europe and the Wehrmacht had begun to stiffen its defenses, Oshima toured the Westwall and the Siegfried Line. He reported on these preparations in great detail in a long radiogram of between 1,000 and 2,000 words.

As a powerful German station pumped it into the ether for the 5,000-mile leap to Tokyo, a new American intercept post at Asmara, in the former Italian colony of Eritrea bordering the Red Sea, picked it up. Back the cryptogram went to the Signal Security Agency. It proved to be in PURPLE, which the American cryptanalysts read with relative ease. The solution went to General Dwight D. Eisenhower's headquarters, where its intelligence helped shape basic strategy for the conquest of Germany.

## 14. Censors, Scramblers, and Spies

CIPHER is the language of spies—and usually they must talk in whispers. A spy's success, his very existence, depends on his not being seen or heard. Sending messages in obviously cryptographic form would alert counterespionage to him as effectively as wearing a cloak and dagger. Yet he must transmit, else he is useless. So he eschews the overt methods of secret communications for the covert. He resorts to open codes, hollow heels, invisible inks, microscopically small missives—the stegano-graphic methods that conceal the very fact that a message is being sent. He seeks to communicate unnoticed.

And to block this very attempt and root out the enemy within, governments erect great filters at their mail and cable ports of entry to prevent and detect these clandestine communications. These sieves, which let innocent messages flow through, are the censorship organizations.

Descended in a sense from the black chambers of the 1700s, they are creatures of war in democracies and of tyranny in dictatorships. Censorship first sprang up on a major scale in World War I, and the lessons that Britain learned then she put to good use twenty years later when

she again filtered communications. Even before the United States entered the war, British censorship had caught two major German spies in the United States and its protectorate of Cuba.

In December, 1940, one of the 1,200 examiners that British censorship had installed in the commodious Princess Hotel in Bermuda stopped a letter addressed to Berlin from New York. He suspected it because it described a list of Allied shipping and used several expressions— such as "cannon" for "guns" in describing the vessels' armament—that suggested the writer might be German and a possible Nazi agent. The letter was signed "Joe K." A watch set up for more letters with his handwriting soon picked out quite a few more, mostly to Spain and Portugal. Their language seemed slightly forced, and a team began studying the letters to see whether this indicated an open code and, if so, what the real meaning was.

One member of the team was a persistent young woman named Nadya Gardner, who became convinced that the letters contained invisible writing. The usual strip tests with chemicals that bring out the ordinary secret inks gave negative results, but Miss Gardner persisted. Finally the chemists, under Dr. Enrique Dent, applied the iodine-vapor test invented back in World War I—and to their surprise secret writing did appear on the back of the typed sheets. The letter of April 15, 1941, addressed to Mr. Manuel Alonso, Apartado 718, Madrid, carried on the back of its two pages a list of ships then docked at New York: "On April 14 was at pier 97 (Manhattan) the Norwegian M. S. *Tain Shan*—6601 tons—gray superstr # at pier 90 was a Dutch freighter. ..." A letter of six days later, addressed to a Miss Isabel Machado Santos in Lisbon, reported in invisible ink that "British have about 70,000 men on Iceland # The S.S. *Ville de Liege* was sunk about April 14—many thanks # Types of airplanes flown to England (continued from letter 69) —3. Boeing B-17c (model 299x) twenty were released by the U.S. Army to Britain on Nov. 20. . . ." These little billets-doux were written in a solution of pyramidon, a powder often used as a headache cure and readily obtainable at most pharmacies.

But there was still no clue as to the sender. The letters bore no return address, and it was rather unlikely that "Joe K" was the spy's real first name and last initial.

Finally, British censorship picked out another Joe K letter that reported that "Phil" had been fatally injured in a New York traffic accident on March 18 and had died at St. Vincent's Hospital. F.B.I, agents found that the man in the accident was known as Julio Lopez Lido, and that witnesses had seen that a man with Lido had grabbed his briefcase after the accident and hurried away. Eventually, the agents learned that Lido's true name was Ulrich von der Osten and that the writer of the Joe K letters was Kurt Frederick Ludwig. Ludwig, born in Ohio but raised in Germany, had come to the United States in March of 1940 to organize a spy ring, which he had done with moderate success.

When captured, he had several bottles of pyramidon in his possession. The odd tone of the open text of his letters was accounted for by its double meanings. "Your order 5 is rather large—and I with my limited facilities and funds shall never be able to fill such an immense order completely," he wrote to one of his addressees—all of them, incidentally, cover addresses for Himmler. This message really meant that he would have difficulty fulfilling the instructions sent him in communication No. 5 because of two few agents and too little money. Ludwig was convicted in the U.S. District Court at Brooklyn.

The second spy trapped by the alert Bermuda station went to his death. On a November day in 1941, an alert censor detected a rather Germanic cast to the handwriting in a Spanish-language letter from Havana to Lisbon and sent it over for a routine test for secret ink. His intuition was confirmed when a long missive appeared, listing ships being loaded in Havana harbor and discussing an airfield being constructed. The examiners were alerted to watch for similar handwriting. The next letter turned up a few days later. Censorship continued picking out these letters, which recited details of merchant shipping in Cuban waters and of the enlargement of the U.S. Navy's base at Guantanamo Bay, until the writer's real Havana address showed up in secret ink. Letters posted to this address were watched, and on September 5, 1942, after sufficient evidence had been amassed, police arrested "R. Castillo," who proved to be Heinz August Luning. He had been sent to Havana from Germany in September, 1941, and of the 48 letters he had sent to Europe, the Bermuda censors had intercepted all but five. On November 9,

1942, he went before a firing squad at Principe Fortress, the first man in Cuba to be executed as a spy.

Soon after Pearl Harbor, the United States built up a censorship service that began in the borrowed office in which Byron Price went to work as Chief Censor and grew to an organization whose 14,462 examiners occupied 90 buildings throughout the country, opened a million pieces of overseas mail a day, listened to innumerable telephone conversations, and scanned movies, magazines, and radio scripts. Millions became familiar with the "Opened by Censor" sticker and the scissored letter.

To plug up as many steganographic channels of communication as possible, the Office of Censorship banned in advance the sending of whole classes of objects or kinds of messages. International chess games by mail were stopped. Crossword puzzles were extracted from letters, for the examiners did not have time to solve them to see if they concealed a secret message, and so were newspaper clippings, which might have spelled out messages by dotting successive letters with secret ink—a modern version of a system described more than 2,000 years earlier by Aeneas the Tactician. Listing of students' grades was tabooed. One letter containing knitting instructions was held up long enough for an examiner to knit a sweater to see if the given sequence of knit two and cast off contained a hidden message like that of Madame Defarge, who knitted into her "shrouds" the names of further enemies of the French Republic, "whose lives the guillotine then surely swallowed up." A stamp bank was maintained at each censorship station; examiners removed loose stamps, which might spell out a code message, and replaced them with others of equal value, but of different number and denomination. Blank paper, often sent from the United States to relatives in paper-short countries, was similarly replaced from a paper bank to obviate secret-ink transmissions. Childish scrawls, sent from proud parents to proud grandparents, were removed because of the possibility of their covering a map. Even lovers' X's, meant as kisses, were heartlessly deleted if censors thought they might be a code.

Censorship cable regulations prohibited sending any text that was unclear to the censor, including numbers unrelated to the text or a personal note in a business communication, and that was not in English, French, Spanish,

or Portuguese plain language. To kill any possible sub rosa message, censors sometimes paraphrased messages. This practice gave rise to Censorship's classic tale, which dates back to World War I. Onto the desk of a censor was placed the cablegram *Father is dead.* The censor considered it briefly, changed it to *Father is deceased,* and forwarded it. Soon thereafter the reply appeared on his desk: *Is Father dead or deceased?*

Cables ordering flowers—"Deliver three white orchids to my wife Saturday"—offered so blatant an invitation to clandestine communication that the censors forbade naming the kind of flower and the date of delivery, leaving both up to the individual florist. Later in the war, all international flower messages were prohibited by the United States' and Great Britain because of the danger of their masking signals. Only those between the U.S. and her territories and between the U.S., Canada, and Mexico were permitted. The censorship permitted only nine of the most widely used commercial codes, and every coded message had to include an indicating abbreviation in its preamble. A firm could not use its private code without a special license from the director of censorship, who required that fifteen copies of the codebook be furnished for use by the censors.*

Precautions were taken with the mass media, too. Newspapers were warned to be careful in taking want ads. Prevention was directed mainly at commercial radio, which could instantaneously deliver open-code secret

*At the start of the war in September, 1939, the Allies prohibited the use of any codes at all. But pressure of business houses and realization that commercially coded messages were only a step up from plaintext forced them to relent, and at the end of December they permitted the use of *Bentley's Complete Phrase Code, Bentley's Second Phrase Code,* the *ABC Code* (6th edition), and *Peterson's Code* (3rd edition). In April, 1940, they admitted five more codes: *Acme Code and Supplement, Lombard General Code, Lombard Shipping Code and Appendix, New Standard Half Word Code,* and *New Standard Three Letter Code.* These were the nine later allowed by the United States and most of the Latin American nations. Under pressure from the Allies, Argentina, which had not severed diplomatic relations with the Axis, halted all code communications—but the first code message stopped was one from the Vatican! During the war, even neutrals such as Spain and Sweden demanded copies of the codes used and prohibited the use of (secret) cipher. Only Switzerland placed no restrictions on either code or cipher communication.

messages to listening submarines or enemy agents with the greatest of ease. Such possibilities had been driven home forcefully to the broadcasting industry a year before Pearl Harbor in a test conducted by a military intelligence officer. By having an announcer mention England's Queen Elizabeth, the officer wove into an interview with former heavyweight champion Max Baer the hidden message: *S-112: Queen Elizabeth sails tonight with hundreds of airplanes for Halifax.* What was disturbing was that neither the announcer, the station manager, Baer, nor any of the thousands of listeners on the nationwide hook-up except those who had been initiated into the secret were aware that the message had been broadcast. With this in mind, the Office of Censorship ruled that telephone or telegraph requests for phonograph records were not to be honored, and that mail requests must be held for an irregular, unspecified time before playing. This would defeat any attempts to have "Jersey Bounce" tell a waiting U-boat that *Convoy sails today.* The same situation applied to the personal ads, such as for lost dogs, that local stations broadcast. Halted completely were man-in-the-street interviews and Santa Claus lists of toys that children wanted.

Preventive censorship like this was only half the job, however. It could not be expected that spies would limit themselves to such easily confounded methods of communication. The other half of the job was the detection of the other methods that they might use. To sharpen Censorship's spy-catching tools by coordinating and assisting the field stations that spotted the hidden messages and by improving liaison with counterespionage agencies like the F.B.I., Price in May of 1943 established the Technical Operations Division at headquarters, appointing Lieutenant Colonel Harold R. Shaw as its chief and an assistant director in the Office of Censorship.

T.O.D. was quartered in the Federal Trade Commission Building, the three-sided structure that housed the Office of Censorship at Pennsylvania and Constitution avenues in Washington. Shaw administered it from Room 509 with three assistants and a secretarial staff. Two technical sections operated under maximum security in a windowless, guarded area on the seventh, or top, floor. The laboratory was headed by Dr. Elwood C. Pierce, a biochemist at the University of Indiana who had joined Censorship at the start of the war. He and his assistant, Dr. Willard Breon

of the University of Maryland chemistry faculty, had prepared a manual on detection of secret inks, trained key personnel of the censorship field stations in laboratory operation, and handled some of the more active and difficult cases themselves. From Hawaii Shaw imported his trusted cryptanalytic expert to form a unit "capable," he said, "not only of cracking codes and ciphers but also of building the intricate dossiers of personal history, contacts, handwriting peculiarities, and correspondence habits of each actual and suspected espionage agent." The man who could do it was Armen Abdian, a former New Englander who had come to Hawaii in the prewar Army, had taught a cram course for prospective West Pointers, and had gone into business in Honolulu.

The primary detection of clandestine communications took place in the censorship field stations. Largest of all was New York's, filling a huge building on Lower Eighth Avenue. About 4,500 postal examiners scanned the snowdrifts of mail that piled onto their desks each day. They excised all matter that might have injured the Allied war effort, and they looked closely for traces of hidden messages. Censorship had catalogued the occupations and hobbies of its examiners. A balance sheet would be given to an accountant to see whether it made financial sense; an amateur horticulturist could tell whether a discussion of tulip beds rang true. Once an examiner in New York was perturbed by a letter from Germany to a prisoner of war in the United States, saying that Gertrude was developing into a swimming champion and listing the times of her victories. He consulted an amateur swimmer in the office, who reported that the speeds were impossible. Further investigation revealed that the times actually indicated the speed of a new-fighter plane, given by a war worker who could not resist bragging. The factory was later bombed. Censors in a political section looked for clues to hoards of vital material that might be bought by the Allies to preclude the Axis from getting it. An economic section extracted remarks about shortages and living conditions to help build up pictures of national economies. Letters in uncommon languages went to a language identification section, which obtained translators for such esoteric tongues as Ladino, a mixture of Hebrew and 15th-century Spanish spoken only by the 30,000 Sephardic Jews in colonies in Spain, the Balkans, and Latin America.

Floor examiners passed all messages with peculiar wording, odd-looking marks, or other suspected indications to the security division, which had two sections to examine steganograms concealed in the two basic ways—linguistically and technologically. These were the code and cipher section for the linguistic steganograms and the laboratory section for the technological. Both were linked to **T.O.D.** by a security assistant who implemented T.O.D.'s instructions and passed the more recalcitrant problems back to Washington. The 70 examiners in the New York code and cipher section occupied about half the 14th floor, with some of the more expert people constituted as a specialist group. About 30 technicians tested for secret inks in the laboratory next door.

Linguistically concealed messages fall into two general categories, the semagram and the open code. There are three kinds of open code: the jargon code, the null cipher, and geometrical systems like the Cardano grille. In the jargon code, an apparently innocuous word stands for the real term in a text contrived to seem as bland and as innocent as possible. Jargon codes can range from the most informal sort of code to a full code list. They begin with mere allusions to mutually known events and persons —"I visited the man you had dinner with last week." They continue through double meanings that would be easily understood by the recipient, as one criminal's referring to another's arrest by saying "Joe went to the hospital." They culminate in a prearranged table of artificial meanings. Jargon has been popular since the dawn of cryptography. The Chinese employed it; the oldest papal code is the 14th-century use of EGYPTIANS for *Ghibellines* and SONS OF ISRAEL for *Guelphs;* in the 17th century a French code consisted entirely of such jargon expressions as GARDEN for *Rome,* ROSE for *the pope,* PLUM TREE for the *Cardinal de Retz,* WINDOW for *Monsieur the king's brother,* and STAIRCASE for the *Marquis de Coeuvres.* It is clear that skillful application of jargon's literary veneer requires no little finesse!

Censorship defends itself against this ruse by a feel for stilted or heavy-handed language and by a healthy skepticism concerning subject matter. The standard story about jargon comes from World War I. A British censor grew suspicious of the enormous orders for cigars wired each day—mostly from port towns—by two "Dutch business-

men." One day Portsmouth called for 10,000 Coronas; the next day Plymouth and Devonport craved large quantities of stogies; then Newcastle succumbed overnight to the tobacco habit. It seemed as though all the males in the coastal population of England had suddenly and simultaneously developed an irresistible addiction to the weed, so inexhaustible was the demand for cigars. At the suggestion of the censor, a check was made; the two businessmen proved to be German spies, and their orders an open code, in which, say 5,000 Coronas for Newcastle meant five cruisers lying in that port. On July 30, 1915, the two—Haicke P. M, Janssen and Wilhelm R. Roos—were executed at the Tower of London by a firing squad whose triggers were really pulled by an alert censor.

A second type of open code is the null cipher. Only certain letters or words of a null cipher's text are significant; for example, every fifth word or the first letter of every word, with all the other letters and words serving as nulls to produce the disguise. These usually sound even more strained than the jargon code. Even two of the better examples, sent by the Germans during World War I, have that "funny" sound that invariably accompanies them. The first, disguised as a press cable, read:

> PRESIDENT'S EMBARGO RULING SHOULD HAVE IMMEDIATE NOTICE. GRAVE SITUATION AFFECTING INTERNATIONAL LAW. STATEMENT FORESHADOWS RUIN OF MANY NEUTRALS. YELLOW JOURNALS UNIFYING NATIONAL EXCITEMENT IMMENSELY.

The initial letters spell out *Pershing sails from N.Y. June 1.* The second message, apparently sent as a check on the first, beaded the same content on the second letters of each word:

> APPARENTLY NEUTRAL'S PROTEST IS THOROUGHLY DISCOUNTED AND IGNORED. ISMAN HARD HIT. BLOCKADE ISSUE AFFECTS PRETEXT FOR EMBARGO ON BYPRODUCTS, EJECTING SUETS AND VEGETABLE OILS.

Whoever the sender was, his ingenuity was expanded in vain, since Pershing actually sailed May 28.

Most null ciphers in World War II were used not by

spies, but by otherwise loyal Americans who could not resist trying to "beat the censor." Servicemen in particular attempted to sneak information about their whereabouts to families who otherwise would quite literally not know where in the world their soldier boy was—even though such attempts endangered the serviceman's own life.

One such system, though elementary, brought deserved bewilderment instead of clarification to its intended recipients. A young GI, following a prearranged system with his parents, tried to tell them he was in Tunis by using first T, then u, then N, i, and s as his father's middle initial in successive letters home. Unfortunately, he forgot to date them and they arrived out of order. The frantic parents wrote that they had looked and looked through their atlas but couldn't find *Nutsi* anywhere! Attempts of this sort grew so frequent by 1943 that the Navy had to warn its sailors that these "family codes," which were usually solved quite easily, could lead to severe penalties for the users.

The third kind of open code is the geometrical. A Cardano grille places the message-bearing words in fixed positions on a page. The significant words can be placed at intersections of the lines of a geometrical diagram of specified dimensions. In the 1600s, Sir John Trevanion, a Cavalier awaiting trial and almost certain execution by Cromwell's forces, noted the third letter after each punctuation mark in a letter that his jailers had scrutinized before giving him arid learned that *Panel at east end of chapel slides.* He disappeared during vespers. And in World War II, captured U-boat officers spelled out secret messages in their letters home by breaking the flow of script after each significant letter. An alert censor noticed that the minute gaps did not occur in natural places, as after syllables. The hidden messages described Allied anti-submarine tactics and technical U-boat faults. Some outlined escape plans— which were, of course, foiled.

The second category of linguistically concealed messages is the semagram (from the Greek "sema," for "sign"). A semagram is a steganogram in which the ciphertext substitutes consist of anything but letters or numbers. The astragal of Aeneas the Tactician, in which yarn passing through holes representing letters carried the secret message, is the oldest known semagram. A box of Mah-Jongg tiles might carry a secret message. So might a drawing in

which two kinds of objects represented the dots and dashes of Morse Code to spell out a message. The New York censorship station once shifted the hands and altered the positions of the individual timepieces in a shipment of watches lest a message be concealed in it.

The examination of the linguistically concealed messages —or, more correctly, those suspected to be such—was largely a frustrating experience. Often the examiner could not tell whether or not a message was hidden beneath the awkward or illiterate or misspelled writing. And even if he felt certain, solution often eluded him. He usually had only one message to work on, and no probable words. Early in the war, censorship practice even forbade working on a suspected cryptogram more than half an hour, on the theory that if the cryptanalyst hadn't gotten it by then, he'd never get it. These unsolved messages posed a difficult problem to the censors. Presumably they were carrying contraband information and so should be banned. But, in the absence of solution, no proof of this existed, and so the letter could not be mutilated. Sometimes this was done anyway, to destroy the suspected code.

Technological steganography early in the war consisted almost exclusively of invisible inks. This is truly an ancient device. Pliny the Elder, in his *Natural History,* written in the first century A.D., told how the "milk" of the tithy-mallus plant could be used as a secret ink. Ovid referred to secret ink in his *Art of Love.* A Greek military scientist, Philo of Byzantium, described the use of a kind of ink made from gall nuts (gallotannic acid), which could be made visible by a solution of what is now called copper sulfate. Qalqashandi described several kinds of invisible ink in his *Subh al-a' sha.* Alberti mentions them. The Renaissance employed them in diplomatic correspondence. About 1530 a book was printed with panels in invisible ink; if these pages were dipped in water, the message would appear; this could be repeated three or four times.

The common inks are of two kinds: organic fluids and sympathetic chemicals. The former, such as urine, milk, vinegar, and fruit juices, can be charred into visibility by gentle heating. Despite their antiquity and their minimal protection, they are so convenient that they were used even during World War II. Count Wilhelm Albrecht von Rautter, a naturalized American who was spying on his

adoptive country for his native Germany, ran out of his good secret ink and had to use urine.

Sympathetic inks are solutions of chemicals that are colorless when dry but that react to form a visible compound when treated with another chemical, called the reagent. For example, when a spy writes in iron sulfate, nothing will be visible until it is painted over with a solution of potassium cyanate, when the two chemicals will combine to form ferric ferrocyanide, or Prussian blue, a particularly lovely hue. The colorless writing of lead sub-acetate will turn into a visible brown compound when moistened with sodium sulfhydrate. Copper sulfate can be developed with ammonia fumes, and it may have been this chemical that was used for the secret writing on the handkerchief of George Dasch, leader of the eight Nazi spies who landed by submarine on Long Island in 1942 to blow up American defense plants, railroad bridges, and canal locks. The red letters that appeared as if by magic when the pungent ammonia reached it spelled out the names and addresses of a mail drop in Lisbon and of two reliable sources for help in the United States. Each of the eight saboteurs had also been given a watertight tube containing four or five matchsticks tipped with a grayish substance that served as a ready-made pen-and-secret-ink. The trick in concocting a good secret ink is to find a substance that will react with the fewest possible chemicals— only one, if possible, thus resulting in what is called a highly "specific" ink.

To test for secret inks, censorship stations "striped" letters. The laboratory assistant drew several brushes, all wired together in a holder and each dipped in a different developer, diagonally across the suspected documents. The developers were wide-spectrum, picking up even such substances as body oils, so that fingerprints and sweat drops often showed up. On the other hand, they missed some specific inks. A bleaching bath removed the stripes. Letters were also checked by infrared and ultraviolet light. Writing in starch, invisible in daylight or under electric light, will fluoresce under ultraviolet. Infrared can differentiate colors indistinguishable in ordinary light and so can pick up, for example, green writing on a green postage stamp. The censorship field stations tested all suspicious letters and a percentage of ordinary mail picked at random, and sometimes all letters to and from a certain

city for a week to see if anything suspicious turned up. During the war, about 4,600 suspicious letters were passed along to the F.B.I, and other investigative agencies; of these 400 proved to be of some importance.

Problems that would not yield to the crude approach of the field stations went back to the T.O.D. laboratory. Here, amid Bunsen burners and retorts, Pierce and Breon, aided by an expert photographer and laboratory technicians, cooked up reagents that would reincarnate the phantom writing. Better equipped and more deeply versed in the nuances of sympathetic inks than the mass-production workers of the field stations, they had received a great stimulus from contact with one of the great secret-ink experts of the world, England's Dr. Stanley W. Collins, who had conducted this battle of the test tubes in two World Wars; he spoke at the Miami Counter-Espionage Conference in August, 1943. T.O.D. soon learned that Nazi spies were taking countermeasures to frustrate the iodine-vapor test and the general reagent.

One was to split a piece of paper, write a secret-ink message on the inner surface, then rejoin the halves. With the ink on the inside, no reagent applied to the outside could develop it! The technique came to light when one German spy used too much ink and the excess soaked through. Sanborn Brown, an M.I.T. physicist, got two inmates of a local jail to explain how two sheets of parchment could be used to do the splitting. They had been caught misapplying the talent to one- and ten-dollar bills, pasting one half of the tens to one half of the ones and passing them with the ten-dollar side up. The method is more an art than a science, for if the sudden tear is not done just right, the paper will shred. To read the message, the paper must be resplit, but it comes apart much more easily the second time.

Another antidetection measure was transfer. German agents would write their message in invisible ink on one sheet of paper, then press this tightly against another sheet. Moisture in the air would carry some of the ink to the second sheet without the telltale differential wetting of the fiber papers on which the iodine test relied. This compelled T.O.D. to find the specific reagent required.

Perhaps the most interesting development of the secret-ink war was the German instrument discovered by Shaw, Pierce, and others in 1945 and dubbed the "Wurlitzer

Organ" because of its resemblance to that musical instrument. They found a burned-out shell of one "organ" in the bombed remnants of the Munich censorship station, and an undamaged one in the censorship station on an upper floor of the Hamburg post office. It examined suspected letters on an assembly-line basis by ingeniously exploiting some principles of physics to make the invisible ink glow. It first exposed the paper to ultraviolet light. This pumped energy into chemicals of the ink, boosting their electrons out of their normal orbits into higher ones. The chemical was then in a metastable state. The heat from a source of infrared then nudged the electrons from their higher orbits back into their regular ones. As they did so, the substance would give up, in the form of visible light, the energy that it had absorbed from the ultraviolet. Since this phenomenon will occur for nearly all substances, even common salt, though some will "naturally shine more brightly than others, the Germans had a system that would develop a good many inks.

The chief difficulty with secret inks was their inability to handle the great volume of information that spies had to transmit in a modern war. One way of channeling large amounts was to dot the meaningful letters in a newspaper with a solution of anthracene in alcohol. This was invisible under normal circumstances but glowed when exposed to ultraviolet light. But with newspapers being carried as third-class mail,' this was hardly the fastest method of getting information to where it was going.

The Germans then came up with what F.B.I. Director J. Edgar Hoover called "the enemy's masterpiece of espionage." This was the microdot, a photograph the size of a printed period that reproduced with perfect clarity a standard-sized typewritten letter. Though microphotographs (of a lesser reduction) had carried messages to beleaguered Paris as far back as 1870, a tip to the F.B.I, in January of 1940 by a double agent, "Watch out for the dots—lots and lots of little dots," threw the bureau into a near panic. Agents feverishly looked everywhere for some evidence of them, but it was not until August of 1941 that a laboratory technician saw a sudden tiny gleam on the surface of an envelope carried by a suspected German agent-—and carefully pried off the first of the microdots, which had been masquerading as a typewritten period.

At first the microdot process involved two steps: A first photograph of an espionage message resulted in an image the size of a postage stamp; the second, made through a reversed microscope, brought it down to less than 0.05 inches in diameter. This negative was developed. Then the spy pressed a hypodermic needle, whose point had been clipped off and its round edge sharpened, into the emulsion like a cookie cutter and lifted out the microdot. Finally the agent inserted it into a cover-text over a period and cemented it there with collodion. Later, one Professor Zapp simplified the process so that most of these operations could be performed mechanically in a cabinet the size of a dispatch case. The microdots, or "pats," as T.O.D. called them, were photographically fixed but were not developed; consequently, the image on them remained latent and the film itself clear. In this less obtrusive form they were pasted onto the gummed surface of envelopes, whose shininess camouflaged their own. The pats could show such fine detail because the aniline dye used as an emulsion would resolve images at the molecular level, whereas the silver compounds ordinarily used in photography resolve only down to the granular level.

The microdots solved the problem of quantity flow of information for the Nazis. Professor Zapp's cabinets were shipped to agents in South America, and soon a flood of material was being sent to Germany disguised as hundreds of periods in telegraph blanks, love letters, business communications, family missives, or sometimes as a strip of the tiny film hidden under a stamp. The very first discovered, and the most frightening, was one in which a spy was asked to discover "Where are being made tests with uranium?" at a time when the United States was fighting to keep secret its development of the atom bomb. The "Mexican microdot ring," which operated from a suburb of Mexico City, microphotographed trade and technical publications that were barred from international channels—a favorite was *Iron Age,* with statistics on American steel production—and sent them to cover addresses in Europe on a wholesale basis, with as many as twenty pats in a single letter. Technical drawings also went by microdot. Other microdots talked of blowing up seized Axis ships in southern harbors, the deficient condition of one of the Panama Canal locks, and so on. Censorship discovered many of these, now that it knew what

to look for, *send* this enabled the F.B.I.'s wartime Latin American branch to break up one Axis spy ring after another.

Telephoning is an exceedingly convenient way to communicate. How delightfully simple to pick up a phone, talk with the other party, and get everything settled in one conversation! Much easier than sending written messages back and forth. But the telephone is notoriously insecure—and its offspring, the radiotelephone, even more so. A single wiretap grants access to a telephone conversation, and only a radio set is needed to overhear radiotelephone talk. And the Axis did not hesitate to grasp these opportunities at the highest diplomatic levels.

The most obvious protective measure against eavesdropping is to make up codes for conversation, and this has of course been done at one time or another by almost anyone who has spoken over the telephone. The codes range from mere oblique references and the most impromptu cant to elaborately prepared lists of jargon. Less frequently, a message might be enciphered in a prearranged system and the ciphertext read off letter by letter, as the Manhattan District did with a checkerboard. Or the speakers may resort to a foreign language.

The United States raised the latter device to the level of a full-scale system in both World Wars by making use of a resource that virtually no other combatant had: pools of tongues so recondite that almost no one else in the world understood them. These were the American Indian languages, which are isolated both geographically and linguistically. In 1918, eight Choctaws of Company D, 141st Infantry, transmitted orders by field telephone; this was the idea of Captain E. W. Horner, who named Solomon Lewis as the chief of the detail. Other Indian tongues were also used. During preparations for World War II, the Signal Corps tested Comanches and Indians from Michigan and Wisconsin in war games, but most of the codetalkers in the combat itself were Navaho. One reason probably was that the tribe was large enough (more than 50,000 persons) to furnish a goodly number of speakers; another, that reportedly only 28 non-Navahos—mainly anthropologists and missionaries—could speak the language, and none of these were German or Japanese; a third reason was the extreme difficulty of the tongue and

the near impossibility—even if someone did learn it—of counterfeiting its sounds.

"Sounds [in Navaho] must be reproduced with pedantic neatness . . . almost as if a robot were talking," wrote anthropologist Clyde Kluckhohn. "The talk of those who have learned Navaho as adults always has a flabby quality to the Navaho ear. They neglect a .slight hesitation a fraction of a second before uttering the stem of the word." A hint of its complexity may be seen in some of its verb forms, on which it insists. The stems of many Navaho verbs differ with the object acted upon. Thus one stem must be used with long objects (pencils, sticks), another with slender flexible objects (snakes, thongs), and still others with granular masses (sugar, salt), things bundled up (hay, bundles of clothing), fabrics (paper, blankets), viscous objects (mud, feces), bulky round objects, container- and- contents, animate objects, and so forth. An entirely different verb form concerns itself with the manner of knowing an event. For example, a Navaho must use one form if he himself is aware of the actual start of rain, another if he believes that rain was falling for some time in his locality before he noticed it, and so on. "Because so much is expressed and implied by the few syllables that make up a single verb form, the Navaho verb is like a tiny imagist poem." Thus "na'fldil" means "You are accustomed to eat plural separable objects one at a time."

A cryptosystem like that boasts considerable security, and it is not surprising that the dark-skinned, black-haired Navaho became a familiar sight in Marine regimental, divisional, or corps command posts, translating a message into a conglomeration of Navaho, American slang, and military terminology as he huddled over a radio set in the Pacific combat zone. Close friends usually worked together. The number of Navaho codetalkers in the Marines rose from 30 at the start of the war to 420 at the end. They relayed operational orders with a secrecy that helped the United States advance from the Solomons to Okinawa.

Linguistic codetalking, jargon codes, or double meanings all use the human speaker as the coding machine. But this job may be delegated to a real machine—the scrambler. These two modes of oral secrecy, the human and the mechanical, correspond to the two basic forms of crypto-systems. Human coding transmutes words, syllables, and

sounds *(as* in Pig Latin)—the linguistic elements of speech —into secret forms and so parallels code. Both ciphers and scramblers, on the other hand, work upon particles of a text cut up without regard to linguistic functions. From this analogy, scrambler methods of modifying speech are called "ciphony" (from "cipher" plus "telephony"). The field of secret voice communication as a whole may be termed "cryptophony."

Though it was only in World War II that scramblers came into widespread use, and only in that war that serious attempts began to be made to solve scrambled speech, devices to assure telephonic secrecy had been in existence almost as long as the telephone itself. The granddaddy of these was patented on December 20, 1881, only five years after Bell obtained his patent on the telephone. Its inventor, 25-year-old James Harris Rogers, an American electrical pioneer who was then chief electrician for the Capitol, wrote: "My invention consists in throwing a message sent from any transmitting instrument through two or more circuits alternately in rapid succession . . . in such a manner that anyone tapping but one of the circuits is unable to obtain anything but a confused and unintelligible series of signals. . . . The two or more lines on which a signal is transmitted according to my plan may be carried to a common terminus by widely different routes, and thus it will be impossible for any person wishing to do so to ... or tap both lines at the same time."

Later methods operate more directly on the speech itself, often in ways that resemble transposition, substitution, and null ciphers. In most of the substitution systems, ciphony selects one component out of the many that make up the complex phenomenon of speech and alters it. It usually chooses frequency, though some scramblers distort volume. Frequency here refers to the number of times the vocal chords vibrate; it is usually stated in terms of cycles per second, or c.p.s., so that a frequency of 500 c.p.s. means that the vocal chords are vibrating 500 times a second. Because of the resonance of the vocal organs, most sounds in speech combine several frequencies, and each sound has its distinctive combination of frequencies. The main frequency of the /e/ sound in "feel," for example, is much higher than that of the /ii/ sound in "fool." Naturally, the absolute frequencies will differ somewhat from Person to person, but it is the relative variations within

an individual's speech that carry much of its information content.

Ciphony seeks to conceal this content by shifting the frequencies of the sounds of speech. It can do this because the telephone first converts these sounds into a fluctuating electrical current, which the tubes, switches, filters, and circuits that comprise a scrambler then modify according to well-known principles of electricity.* Though this current may be, transformed in a great variety of ways, many affect the voice essentially alike, so that there are relatively few basic scrambles.

The simplest is inversion. This turns the voice upside down. Though normal speech ranges from about 70 to about 7,000 c.p.s., the telephone, for engineering reasons, responds only to sounds from about 300 to 3,300 c.p.s. It is this frequency band that is inverted. A voice tone of 300 c.p.s. will emerge from the inverter at 3,300 c.p.s., and vice versa. A tone of 750 c.p.s. will become 2,250 c.p.s., and again vice versa. It is the equivalent of *a* = *z,*

*b* = Y.....*z* = A, a phonetic atbash. Inverted speech

sounds like a thin high-pitched squawking, ringing with bell-like chimes. The word *company* resembles CRINKAN-OPE, *Chicago,* SIKAYBEE. The inversion pivots in the middle of the frequency band, which means that tones in this area somersault through a narrow range. A frequency of 1,625 will become 1,675. This relative lack of change results in the phenomenon that the word *inverter* itself, which is composed largely of such tones, emerges from the enciphering process that it describes almost unchanged!

Another simple technique is the band-shift. This is a kind of telephonic Caesar substitution, in which all the frequencies are shoved upwards or downwards a certain distance, with the portion pushed out of the frequency band reentering at the bottom or the top. For example, a factor of 1,000 might be added to all frequencies in the 300-to-3,300 band, so that a tone of 500 c.p.s. would be

*It does not seem possible to devise a scrambler that distorts the sound itself (i.e., the vibrations in the air) because, once the waves were degraded by, say, some kind of baffle, they could not be restored to their original form. Transposition systems, on the other hand, might be possible in a very crude form by means of mechanical phonographs. From a practical point of view, however, nonelectrical scramblers may be ruled out. None ever seems to have been constructed.

tJtlNSUKS, S^KAJVLBLtKB, **AIN1J**

shifted *to 1,500. One of 2,800* c.p.s. would then be enciphered to 800.

Band-splitting splits the frequency band into several smaller bands and interchanges these. Filters can divide a 250-to-3,000 band into five subbands of 550 cycles each: subband A of 250 to 800, subband B of 800 to 1,350, subband c of 1,350 to 1,900, subband D of 1,900 to 2,450, and subband E of 2,450 to 3,000. Then the scrambler's switches and circuits may replace A by c, B by D, c by E, D by A, and E by B, thus jumbling the normal tones. The better band-splitters shift these substitutions every few seconds or milliseconds. The result sounds something like a recording of a Mah-Jongg game played too fast.

Masking systems bury the voice signal in noise. The music from a phonograph record can be electrically superimposed on the voice, drowning it out. The descrambler, which must have an identical disk precisely synchronized with that of the scrambler, subtracts the phonograph signal out, leaving the voice. These systems resemble null ciphers, which interlard the true message within a welter of spurious symbols. Another system is wave-form modification. A fluctuating electrical current operates upon the voice current to produce rapid and extreme variations in the amplitude of the transmitted speech. This sounds rather like a radio whose volume control is being turned up to full blast one instant and then down to a whisper the next. In the descrambler, an identical synchronized current reverses these effects.

All these encipherments transform the speech only in the frequency dimension, along the vertical axis, as it were. None extends horizontally along the time axis. Systems that encipher by changing the temporal relationships of speech's continuous flow must preserve it momentarily to permit the transposition. Usually they have used magnetic tape.

Time-division scramble, or T.D.S., chops the stream of speech into split-second portions and shuffles them. It does so by tape-recording the voice and then picking off segments in jumbled order, using, say, five pickup heads fhat a mechanism activates in mixed sequence. The result [18] a literal hash of sounds. The descrambler uses five recording heads to lay the sounds back on a moving tape m their proper order. Another tape-based scramble, the

wobble, slides a pickup head back and forth along ft,; length of the tape as the tape passes beneath it. As tK: head moves opposite to the tape's direction, it will re off the signals faster than, they were recorded, and the ; will sound higher than normal. As the head moves wi the tape, it will read off the signals more slowly than tht were recorded, and these will sound lower than norm, \ The result will be an alternation of squeaks and grow-sounding exactly as if a phonograph record were alternately raced and almost stopped.

Most of the basic scrambler systems were invented during the 1920s and 1930s by engineers for the growing radio and telephone companies. A need for them first became apparent when the radio hams began listening in to the conversations of erring husbands and their wives and on stockbrokers giving tips on the first public radiotelephone service, offered after World War I by the Pacific Telephone Company between Los Angeles and nearby Catalina Island. The American Telephone & Telegraph Company installed an inverter. While it prevented casual eavesdropping, it would not keep a determined amateur from inverting the inversion. And several did just that on the East Coast in the latter 1920s when the telephone company was setting up its radiotelephone link to Europe. Among them was a young man of 20, William Roberts of Trenton, who even sold some of his "De-Scramblers" to Latin American countries.

Growing realization of the insecurity of the inverter caused its replacement by band-splitters on both the A. T. & T. transatlantic radiotelephone circuit and the Radio Corporation of America's circuit between San Francisco, Honolulu, and Tokyo. Called the A-3, this Bell Telephone device not only switched the substitution assignments for its five subbands but inverted them as well. However, of the 3,840 possible combinations, only 11 were considered suitable for privacy, and of these only 6 were actually used. They were brought into play in a cycle of 36 steps, each of which remained for 20 seconds, giving the A-3 an overall period of 12 minutes. It began operating betwee the R.C.A. post in San Francisco and the Mutual Tel-phone Company post in Honolulu in December, 1937-and a few days later the Tokyo post, which was still using the old inverters, asked what kind of system was in use on the other leg of the circuit, since they could not understand

it. The military took the query as proof that Japan was monitoring the mainland communications.

It was the A-3 that brought news of World War II to President Roosevelt, who was awakened early on the morning of September 1, 1939, by a call from the American ambassador in Paris, William *C.* Bullitt. As the United States was drawn closer and closer to war, the President conferred with his emissaries abroad more and more by scrambler radiotelephone. During the Battle of France he sometimes spoke with Bullittt several times a day. Characteristically, Roosevelt liked the telephone because it cut through the red tape of diplomatic routine and the delays of coding and cabling and because it gave him personal contact with the speaker. Occasionally he spoke' with Premier Paul Reynaud, and frequently and increasingly with Churchill.

The President's words sped from the White House to the overseas switchboard in an A. T. & T. building at 47 Walker Street, New York. In common with all other transatlantic conversations, the nasal Roosevelt drawl then entered a special locked room, barred to all except government-licensed employees, where the A-3 equipment mangled it. Here engineers watched dials and listened to the sound to make sure that the speech was properly scrambled. At the transmitter, channel mixers continually shifted the transmission from one frequency to another, so that anyone listening on one circuit would hear it go suddenly blank.

And someone was indeed listening. The Deutsche Reichspost—which, like other European post offices, handled telephone and telegraph traffic as well as mail—-realized that the only telephone link between England and the United States was the radio circuit, and it reported "The special national political importance of this communication connection has caused the D.R.P. to try with all available scientific means to decipher the conversation carried on this connection." A task force under Postal Counselor Graduate Engineer Vetterlein of the D.R.P.'s Forschungsanstalt ("Research Bureau") set to Work on the problem. The engineers soon learned the nature of the A-3 system and found that they had to wire circuits for only the six different combinations of subband substitutions. Naturally, they had to experiment to find the exact subband divisions and the sequence in which

I

the *six.* combinations were used, but from start to finish the solution took only a few months. They completed it by September, 1941. Within a few more months the D.R.P. had established an intercept and voice-cryptanalysis station on the Dutch coast. Its elaborate equipment instantaneously unscrambled the conversations, losing only a syllable or two after a key change until the proper one was found. When this was in operation, the German Postal Minister, Wilhelm Ohnesorge, notified Adolf Hitler:

THE REICHSPOST MINISTER — BERLIN W 66,
6 March 1942
LEIPZIGER STR. 15

U5342-1/1 Bfb Nr. 23 gRs SECRET REICH MATTER

Decipherment of the U.S.A.-England telephone connection

Mein Führer!

The Forschungsanstalt of the Deutsche Reichspost has completed as the latest of its enterprises an intercept installation for the telephone traffic between the U.S.A. and England, which has been made unintelligible using all present knowledge of communications technology. Thanks to the devoted work of its scientists, it [the D.R.P.] is the only place in Germany that has succeeded in making the scramble, which had been made unintelligible with the best methods, again understandable at the instant of its reception.

I will give the results of our interceptions to the Reich Leader of the S.S., Party Comrade Himmler, who will submit them on March 22.

I will limit the circulation of this communication pending higher decision in view of the fact that if this success were to come to the knowledge of the English, they would further complicate the problem of telephone traffic and cause it to be sent on the telegraph cable.

Heil mein Führer!
*(signed)* Ohnesorge

To the
Leader and Reich Chancellor o
f the Greater German Reich
Berlin W8

Dr. Ohnesorge appended a concrete example of the intercept station's success: a cryptanalyzed and translated conversation plucked from the ether at 7:45 p.m. September 7, 1941. A Briton who had just arrived in the United States was talking with a colleague back in England about the need for a man named Campbell to have an assistant and about their propaganda bureau.

The group continued to send transcripts to Hitler's desk, including a 1942 chat between Churchill (at Whitehall 4433) and a Mr. Butcher in New York, and one between Major General Mark Clark and the Inspector General's office in Washington.

[Codebreakers 297.jpg]

*Transcript of a German descrambling of an intercepted Churchill transatlantic conversation*

At 1:00 a.m. July 29, 1943, they hit the jackpot: a radiotelephone conversation between Roosevelt and Churchill. They were discussing the coup in Italy that had just ousted Mussolini's government:

"We do not want proposals for an armistice to be made before we have been definitely approached," said Churchill.

"That is right," agreed Roosevelt.

"We can also wait quietly for one or two days."

"That is right," said Roosevelt again.

Churchill said that he would contact the king of Italy, and Roosevelt replied that he too would get in touch with "Emmanuel." "I do not know quite how I shall do this," he admitted. The Germans took the conversation as evidence of the treachery and complicity of the Italians: "This is complete proof that secret negotiations between the Anglo-Americans and Italy are under way," the war diary of the O.K.W. noted. This does not seem to have been the case; in any event, the Allies were cool to the coup.

Later the Forschungsanstalt again picked up a Roosevelt-Churchill conversation—Churchill was practically addicted to the telephone, calling Roosevelt at all hours from his bombproof shelter in Whitehall, and placing great faith in the scrambler. This conversation, early in 1944, "lasted almost five minutes," wrote Walter Schellenberg, the Himmler aide who studied it, "and disclosed a crescendo of military activity in Britain, thereby corroborating the many reports of impending invasion." Soon thereafter the A-3 was replaced by a more secure system, and English became Greek to the listening Germans.

## 15. The Scrutable Orientals

FROM THE SUNDAY morning when Commander Mitsuo Fuchida, in his bomber high over Pearl Harbor, radioed "TORA, TORA, TORA!" to indicate that his attack force had achieved complete surprise, the gods of war had smiled without surcease upon the armed forces of imperial Japan. The strike at Pearl Harbor had decimated the United States fleet. Unhindered, the Greater East Asia Co-

Prosperity Sphere expanded rapidly and uninterruptedly. Guam was captured on December 10, Wake on the 23rd. Two days later Hong Kong fell. Japanese aircraft sank *Prince of Wales* and *Repulse,* giving Winston Churchill his worst shock of the war and leaving the whole western Pacific, the Indian Ocean, Oceania, and even Australia virtually undefended by naval forces. Tojo's armies overran Singapore and Malaya with its rubber plantations, then the Dutch East Indies with its great oil fields. Siam and the Solomons were in their hands. China was under blockade. In May the Philippines surrendered. Within six stupefying months, the Rising Sun shone upon nearly a tenth of the globe's surface. Nippon's enemies had been wiped from the seas. Her troops raped and pillaged from bustling Rangoon to the languorous South Sea islands. It was the most rapid conquest in history.

It amply fulfilled the Japanese war plan. Japan did not intend to invade the United States. Rather, she planned to feed upon the riches of the conquered territories behind a ring of impregnable defense positions, from which she would beat off any attacker. But the high command, bedazzled by success and greedy for more, decided instead to continue the sweep before its momentum was lost. The admirals and generals pointed out that naval losses, which they had anticipated at 25 per cent, had been infinitesimal. The largest ship sunk had been a destroyer, and so more than adequate forces remained for the new drive. Furthermore, they reasoned, the defense perimeter would be protected as much by greater depth as by greater consolidation. They therefore set in motion two ambitious plans. One was an amphibious assault southward to Port Moresby, a town on the southeastern tip of New Guinea only 400 miles from Australia. The other pivoted on Midway, a tiny atoll in the middle of the Pacific that stood as a sentinel to Hawaii.

This second plan had two parts. The first part aimed at the atoll's capture. Its two coral islets—the larger barely two miles long—possessed no intrinsic worth but great strategic value, for whoever held them controlled the central Pacific and hence the approaches to either end of the oceanic basin. The second and more important part of the plan sought to lure out the remainder of the American fleet and destroy it. Admiral Isoroku Yamamoto, Commander in Chief of Japan's Combined Fleet, appreciated

America's industrial might and realized that Japan had to win quickly—before America could bring it to bear. He also knew that the United States could not let Midway go by default, as it had Wake and Guam. When the Pacific Fleet, enfeebled by the losses at Pearl Harbor, steamed out to defend the atoll, he would fall upon it with his vastly superior forces and annihilate it. This final disaster would convince Americans that Japan could not be beaten. They would therefore quit a pointless struggle and leave Japan master of the western Pacific. Or so the warlords purposed.

They did not know that the United States had fashioned a secret weapon of such potency that it could alter the balance of power in the Pacific. It was located in the long, narrow, windowless basement of the 14th Naval District's Administration Building in the Navy yard at Pearl Harbor. VaultHke doors protected its secrets; steel-barred gates at the top and bottom of the stairs kept out visitors; guards stood a round-the-clock watch. This office was staffed, when the war broke out, with about *30* officers and men. It was equipped with International Business Machine Corporation tabulators, which were partitioned off in a separate section because of the racket they made. Its raw material came in by courier from the radio intercept station at Wailupe. This was the so-called Combat Intelligence Unit, the radio intelligence organization that served the Pacific Fleet.

Lieutenant Commander Joseph John Rochefort had commanded it since May of 1941. Before Pearl Harbor, the bulk of its personnel worked on interception, direction-finding, and traffic analysis; the unit fed these results to the fleet intelligence officer. Though one of its young crypt-analysts, Chief Radioman Farnsley C. Woodward, had attacked the Japanese diplomatic systems in use by the Honolulu consulate as a favor for counterintelligence, the unit's main cryptanalytic duties before Pearl Harbor involved the solution of the Japanese flag officers' system and miscellaneous administrative, personnel, and meteorological codes. It had only three real cryptanalysts to handle this workload, Rochefort and Lieutenant Commanders Thomas H. Dyer and Wesley A. Wright. The others were trainees, aides, clerks, and translators. Since August of 1941 it had been working a seven-day week; in October it

went to a night watch as well—the only unit in Pearl to do so.

Three days after Pearl Harbor the unit was given a major change in assignment. It was to discontinue work on the flag officers' system (which was to be analyzed in OP-20-o in the Navy Department in Washington) and to join in the attack and breakdown of the Japanese fleet cryptographic system, dubbed JN25 by OP-20-G. This most widely distributed and extensively used of Japan's naval cryptosystems, in which about half her naval messages were transmitted, was already the target of three other cryptanalytical units—a 16th Naval District group under Lieutenant Rudolph J. Fabian on Corregidor, a British group at Singapore, and OP-20-o. They had determined that it was a two-part code of about 45,000 five-digit groups, enciphered by two volumes of 50,000 five-digit additives each. The b, or second, edition had come into force on December 1, 1940, and by the following November messages in it were partly readable. At 6 a.m. on December 4, 1941, new additive books came into effect, together with new indicators. Fabian's group broke into this new encipherment four days later, and by Christmas messages were again being read as before. But these readings were tantalizingly fragmentary, and much remained to be done.

The commencement of hostilities generated an enormous increase in radio traffic and consequently in the workload of the Combat Intelligence Unit. To handle it, the unit dragooned personnel from every possible source. It first acquired the band of the U.S.S. *California,* which had been badly damaged in the first few minutes of the air attack. Dyer threw up his hands when he heard about it, but music and mathematics and cryptanalysis seemed to go together,* and nearly all the bandsmen proved above average and some exceptional in their new tasks. By May, the basement office contained about 120 persons. Of these, perhaps half a dozen were by then fairly competent crypt-analysts, 50 were beginning to get the feel of the work, and the remainder were clerks. Work went on round the clock in the air-conditioned basement, but the unit was woefully understaffed.

*As corroboration, it might be noted that Painvin won a prize as a young 'cello player, that Mauborgne and Kunze both play the violin at least passably, and that an English expert taught music.

Rochefort virtually lived in that cellar for the first three months. He supervised the entire operation—interception, traffic analysis, cryptanalysis, translation. Dyer, his immediate subordinate, was in charge of the cryptanalytic section. A slender man just turning 40, with a mild, friendly personality but a tough and unrelenting mind, Dyer had come to the Islands in 1936 and had begun cryptanalytical work largely on his own initiative. He had become interested in the field soon after his graduation from Annapolis in 1924. Assigned to *New Mexico* as an assistant radio officer, he began doing the cryptograms in the naval communications bulletins, which intrigued him, and then read Friedman's *Elements of Cryptanalysis,* which hooked him. In 1931, he succeeded Safford as head of the Research Desk in the Code and Signal Section of Naval Communications, commanding the entire U.S. Navy crypt-analytical group of four people, clerks included.

The following year, Dyer became the father of machine cryptanalysis when he installed I.B.M. machines to speed up solution. (The Army did not begin using the machines for cryptology until 1936.) In 1937, after he had been in Hawaii for a year, the Navy sent some I.B.M. machines out to him and assigned him a yeoman to expand, in a modest way, the cryptanalysis that he had been doing. Those machines were his baby. While other cryptanalysts used pencil and paper to test assumptions, Dyer tried them out directly on the machines—and worked more quickly that way than he could have by hand. He stayed in cryptanalysis all during the war, winning the Distinguished Service Medal, and even afterward, rising to a captaincy. On his retirement from the service in 1955, he started teaching mathematics at the University of Maryland.

His chief assistant was Wright, who handed out the work that Dyer wanted done and then pitched in himself. In 1929, three years after he graduated from Annapolis, he found himself with his crew on a rifle range shared by Safford, a fellow officer in a destroyer division. Like Dyer, he had solved the ciphers in the communications bulletins, and Safford, in a sales campaign that began to the crack of musketry, convinced him that he should specialize in cryptology. But it was not until June of 1933 that Wright began his first tour in communications. Sea duty alternated with cryptologic work until, in March of 1941, he went to Pearl Harbor with Admiral Kimmel as the cryptanalyst in

*a.* fleet security unit. He immediately began working with the Combat Intelligence Unit and in February of 1942 was formally transferred to it. He was then 39, a broad-shouldered redhead with craggy features and big hands whose strong resemblance to a tugboat captain—his nickname is "Ham"—belies his gentle manner and his courtesy. He too remained in cryptology throughout the war, winning the Legion of Merit; like Dyer he stayed in it afterwards, winning a gold star to his Legion of Merit. He retired in 1957.

With the entrance of the Rochefort group into the fray against jN25b, the three Allied cryptanalytic units in the Pacific and OP-20-G in Washington began working in the closest possible cooperation. Positive or tentative codegroup recoveries were flashed from unit to unit via the intercept channel for MAGIC. Each unit intercepted messages that the others might not have picked' up, and so could make new assumptions or confirm or disprove old ones. Washington, which had the most equipment and the largest staff, seems to have led in the work of stripping the additive groups. The Singapore and the Philippines units had made the difficult initial entries, but their work was interrupted when the British had to move to Colombo and Fabian was evacuated by submarine from Corregidor in February, 1942, several weeks before MacArthur. Aside from a few such generalized observations, it is almost impossible to say which group, much less which individual, deserves the major share of credit for solving the edition of the fleet cryptographic system then in force. Collaboration was too intimate. A possibility raised in a discussion between Dyer and Wright might be developed into a probability by a check of messages in Washington and verified by a new intercept at Colombo.

Meanwhile, the Japanese—who had no suspicion of all this activity—felt a vague unease at the extreme length of service of this code. A new edition, which would be called JN25c by the Americans but was called the Naval Code Book D by the Japanese, was to be placed in service April 1. But administrative confusion in the Navy libraries, which had custody of the codebooks, plus difficulties in physically distributing the books by destroyer and airplane to moving ships and widely dispersed installations, forced a postponement to May 1. Consequently, the American cryptanalysts could tunnel ever more deeply into JN25b.

Gradually the isolated fragments of plaintext that they were recovering grew denser, enlarged, touched, made sense. Parts remained unread, but the large patches of coherence offered clues to Japanese thoughts and plans. Hence it was that by April 17 the cryptanalysts smoked out the gist of the Japanese plan to seize Port Moresby and threaten Australia. The new Commander in Chief of the Pacific Fleet, Admiral Chester W. Nimitz, dispatched two carriers, *Lexington* and *Yorktown,* to spoil it.

This task force, commanded by Rear Admiral Frank Jack Fletcher, began cruising the lovely waters of the Coral Sea off the northeast coast of Australia in search of the enemy. At 8:15 a.m. May 7 a message from a *Yorktown* search plane was decoded as reporting the discovery of "•two carriers and four heavy cruisers" 175 miles northwest of the American force. Fletcher thought that this was the main Japanese force covering the amphibious landing and flew off two deckloads of planes to attack it. When the search pilot returned, it was discovered that the "two carriers and four heavy cruisers" had resulted from a disarrangement of his codepad; they should have been reported as "two heavy cruisers and two destroyers." But another contact report alerted the fliers to the presence nearby of the landing force itself, escorted by the light carrier *Shoho.* They swarmed over *Shoho* and sank it in ten minutes—a record for the war. "Scratch one flattop!" exulted one pilot. The transports, shorn of their air cover, retired to the northward. This accidental attack on the wrong force thwarted the main Japanese objective and, since the transports never again entered the Coral Sea, lifted the threat of invasion from Australia.

Fletcher could hardly foresee this, however, and next day he located the main Japanese force of two big carriers and attacked them at the same time that they spotted and attacked him. It was the first naval battle in history which was fought entirely by air and in which the opposing ships never even sighted each other. One Japanese carrier was put out of action; the other had its flight deck bent so that it could not recover all its planes, many of which had to be jettisoned. But *Yorktown* was scarred and the beloved *Lexington* so badly damaged that, after futile attempts to save her, she had to be torpedoed by an American destroyer. Though this gave the Japanese a tactical victory in the Coral Sea, they had lost strategically. More important,

their two damaged carriers would not be present at the Midway battle. For the check at the Coral Sea had not altered Japan's grandiose plans for winning the war against America.

During these hectic spring days, the cryptanalysts strained under high pressure. Rochefort and Dyer alternated 12 hours on, 12 hours off. Speed was emphasized. As the meaning of a codegroup became known in the Combat Intelligence Unit, whether through its own efforts or by a helpful message from another unit, the codegroup and its meaning were punched on an I.B.M. card and stored in the machine. When an intercept came in, a clerk would punch its codegroups on I.B.M. cards and feed them in. The machine automatically made the run of repeated subtractions and the check of its mechanized difference "books" necessary to find the identical remainders, and then, with human guidance, the runs to reconstruct the relative additive sequence, correct it to the absolute sequence, and strip it from the encicode message. This machine would then compare the placode groups with the decode cards in its storage and print out the plaintext for whatever decode cards it had. Presumably it would also print out the various possibilities in the case of garbled or partial codegroups. It could also make frequency counts and contact counts and on command could disgorge a desired set of statistics—all codegroups preceding and following a given codegroup, for example. Head of the I.B.M. room, which was constantly being enlarged, was Lieutenant Commander Jack S. Holtwick, Jr., a 1927 Annapolis graduate who had done cryptologic work at the Navy Department, the 16th Naval District, and the Asiatic Fleet from 1934 to 1939; he had reported to the Hawaiian unit in June of 1940.

Not every cryptogram was decrypted. Japanese traffic was too heavy for the undermanned Combat Intelligence Unit. All major and most minor Japanese fleet circuits were monitored, and the messages that were driven down by car from the intercept stations were scrutinized by traffic analysts. From such indications as the length of a message, its originator, the time of day at which it was sent, the circuit used, the addressees, and stereotypes in the text of the cryptogram itself, plus an intuitive "feel" based on day-in, day-out listening-in to Japanese communications, these "scanners" could pick out the important messages.

The cryptanalysts concentrated on these, filling in missing additives and conjecturing the meaning of new codegroups. They seldom read messages "solid"; even the translators— who were half cryptanalysts—did not fill in all the holes.

As these translations were written up, Lieutenant Commander W. J. (Jasper) Holmes brought them, blank spots and all, together with some that were very sketchy indeed, to Nimitz' chief of staff, Rear Admiral Milo F. Draemel, who took the important ones in to Nimitz himself. Holmes had retired in 1936 with an arthritic back but had returned to active service after Pearl Harbor. He was a good enough writer to have sold several pieces on naval subjects to *The Saturday Evening Post,* the toughest magazine market in America, and he used this literary ability in collaborating with the fleet intelligence officer in pulling together information from sightings by U.S. submarines, traffic analysis, and comparison of many intercepts into an intelligence compendium that went to the higher-ups.

On May 5,* Imperial General Headquarters issued Navy Order 18: "Commander in Chief Combined Fleet will, in cooperation with the Army, invade and occupy strategic points in the Western Aleutians and Midway Island." Wireless traffic subtly changed its character. More than 200 ships would take part in the operation, and though most were already in the Inland Sea, many of the carriers, battleships, submarines, minesweepers, transports, and supply vessels had to be summoned from missions at sea. Some had to be refitted, and messages crackled to and from the naval base at Kure. The magnitude of the supply problem alone was indicated by the fact that this one operation would consume more fuel and cover a greater mileage than the entire Japanese Navy had done in any previous peacetime year. The battle preparations called for the ships to assemble in Hiroshima Bay and then to sortie in five main forces over a four-day period according to a precisely calculated schedule. The directives, queries, and responses involved in organizing so complex an operation filled the airwaves. Coded messages streamed out of Yamamoto's headquarters aboard *Yamato,* the world's largest battleship. And not only the legitimate recipients were reading them.

For the effective date of the new edition of the fleet cryptographic system, which had been postponed once

*A11 times are local times. This would be May 4 in Hawaii.

from April 1 to May 1, had to be again set back another month, to June 1. Perhaps the very extent of the Japanese conquests defeated their distribution efforts. These may not have been very energetic in any case, for the Japanese, while paying lip service to the need for communication security, seemed to believe, on the evidence of their military successes, that their codes were not being broken and that timeliness in their replacement was not really necessary. By early May, Allied cryptanalysts, who had recovered about a third of the JN25b lexicon, could read about 90 per cent of an ordinary cryptogram (because the recovered codegroups were the most frequently used). Had Japan changed her main naval code on May 1 as scheduled, she would have blacked out Allied cryptanalysts for at least several weeks—weeks that, as it turned out, were to be crucial to history.

Her failure to do so meant that she was masking her Midway preparation messages behind a cryptographic smoke screen that American cryptanalysts had almost entirely blown away. And as solutions of these messages drifted into Nimitz' office in the first weeks of May, that old sea dog scented a major offensive. Hastily, he recalled carriers *Hornet* and *Enterprise,* which had headed for the Coral Sea after launching Jimmy Doolittle's raid on Tokyo, and *Yorktown,* to be ready for any eventuality. But what eventualities were possible? The Fleet Intelligence Summary of May 15 warned of an enemy raid or seizure of Dutch Harbor in the Aleutians some time between May 30 and June 10. This was almost certainly a diversionary move. But where would the main Japanese attack fall—and when? There was no clear-cut answer. Several Japanese strategies appeared possible. Nimitz himself thought Midway was the target, but in Washington Admiral Ernest J. King, Chief of Naval Operations, who was working from essentially the same information, concluded that Oahu was.

Yamamoto was well aware of the inestimable advantage of surprise, that element of warfare which so often decides the course of battle. He felt confident that the United States, unable to defend all points, would have to counterattack at a time and place governed by the Japanese moves, giving Yamamoto control of every situation. In addition to this tactical initiative, he had an overwhelming preponderance of forces. To his 11 battleships, 5 carriers, 16 cruisers, and 49 destroyers, Nimitz could oppose no battle-

ships and only 3 carriers, 8 cruisers, and 14 destroyers.

On May 20, Yamamoto issued an operations order that spelled out in detail the tactics to be used in the Midway assault. It was to begin on June 3 with a diversionary attack on the Aleutians. With Nimitz' forces thus pulled off balance, the softening-up would begin on the Midway defenders, to be followed on June 6 by a dawn assault. When the Pacific Fleet either hurried south from the Aleutians or sallied forth from Pearl Harbor to defend Midway, the numerically superior bombers and torpedo planes of the Japanese force would cripple it. Then Yama-motb's battleships and heavy cruisers would move up to sink its remnants by gunfire. The work of December 7 would be completed; a Japanese Midway would rule the Pacific, threatening Hawaii itself; and the war would be as good as won.

Unknown to Yamamoto, his order was also picked up by the Allied listening posts that ringed the Pacific. Its extreme length indicated its importance, and Fabian's unit, by this time in Melbourne, may have first suggested that it might be an operations order. But the Hawaii unit put out the first fragmentary solution. The I.B.M. apparatus rapped it out in a mechanical cryptanalysis for as much of the intercept as codegroups and additives were available in storage. Only about 10 to 15 percent of the message was lacking, and the unit began a massive effort to fill in these holes. This task lasted more than a week. Dyer pushed cards through the clacking machines. The. fledgling crypt-analysts drove pencils furiously across sheet after sheet of paper. The clerks scurried among the desks. Overworked language officers sucked in Japanese through their eyes and spouted English at their fingertips. Gradually additives were recovered and stripped and the plaintext of the uncovered codegroups was revealed or inserted. As each new portion came to light, adding another scrap of information, it was rushed upstairs to Jasper Holmes. He would write it into its proper place in the picture and send it along to Commander Edwin T. Layton, the fleet intelligence officer, for transmission to Draemel and Nimitz. The operations order was so long and so detailed that dozens of such fragments rustled across the commander's desk.

Still in doubt, however, were its most important parts: the dates, the times, and the places of the various operations. The date-time information had been superenciphered

in what appeared to be a polyalphabetic system. This had never been solved because it had been observed only three times before, and one occasion had a garble that threw sand in the gears of every attempted reconstruction. The crypt-analysts had considered that they could not do anything with this, and so, rather than waste a man on a fruitless endeavor, all hands concentrated on the body of the message. Additives and codegroups recovered there would be of value in later solutions. Consequently, the question of when was left to other branches of naval intelligence, which applied ship speeds and similar data to estimate the date and time for the attack.

The question of where was answered fairly quickly by the Combat Intelligence Unit. The Japanese indicated geographic locations by maps with coordinates in code; they called these their CHI-HE systems, and they served as much to avoid error in transliterating kata kana as to conceal. The cryptanalysts had partly recovered one such map; they knew the designators for Pearl Harbor, for example. Several weeks earlier, they had discovered the code coordinates AF in a message sent from two scout planes over Midway. Context suggested that AF meant *Midway.* When they checked this against their partially solved map grid, they found that A'S representing one coordinate of Midway's position and F'S representing the other fit into it perfectly. So when they saw that AF was the codegroup for the locus of the main attack, they felt quite sure that Midway was the target.

But the top brass squinted at this identification. On it rode the very existence of the American fleet and the future course of the whole Pacific war. They demanded confirmation.

Rochefort decided to trick the Japanese into giving him the proof. He cooked up the idea of having the Midway garrison broadcast a distinctive plain language message which would presumably be picked up by Japanese monitors. Their coded report would be intercepted and solved by Americans, and the geographic indicator that they used in this telltale dispatch would have to mean *Midway.* Layton liked the idea, and the two men drafted a message in which Midway reported that its fresh-water distillation Plant had broken down. They cabled it to the atoll with an order to radio it back to Pearl in clear. Midway complied. The cryptanalysts waited. Two days later there appeared in

the harvest of Japanese intercepts one stating that AF was short of fresh water.

By about Wednesday, May 27, Nimitz knew almost as much about the Midway operation as many of the captains of Japanese warships who were to take part in it. In all respects but one his information was solid: it had come from the Japanese themselves and had even been verified. The one point was the when. His intelligence staff had erected an elaborate scaffolding of estimates, deductions, probabilities, and predictions to date the operation as beginning against Midway June 3. The reasoning was shrewd, but its hypothetical framework could hardly have comforted Nimitz in so weighty a matter as much as the repeatedly confirmed perceptions of the cryptanalysts.

Meanwhile, in the basement office, nearly everything that could be done to the body of the Yamamoto operations order had been done. Hardly any gaps remained, and only an occasional paper went upstairs. Intercept importance had fallen off with the sortie of the Japanese fleet under radio silence. Late one afternoon in this comparative lull, Lieutenant Commander Joseph Finnegan, a 1929 Annapolis graduate who had served as a language officer in Japan from 1934 to 1937, brought the section with the untouched internal date-time cipher over to Wright.

"Ham," he said, "we're stuck on the date and time."

Wright had already stood his 12-hour watch and was about to go home before returning in 12 hours for another. Instead, he went with Finnegan to an empty desk in the traffic analysis section. Finnegan gave him the three previous uses of the cipher—one of them in a message that had led to the Coral Sea battle, another the garbled text. Wright put four people on a search for other instances of the cipher, and he and Finnegan set to work. For a good while the flaw in the one corrupt cryptogram frustrated their efforts, but as the night wore on Wright worked it out. He discovered that the date-and-time cipher comprised a poly-alphabetic with independent mixed-cipher alphabets and with the exterior plain and key alphabets in two different systems of Japanese syllabic writing—one the older, formal kata kana, the other the cursive hira gana. Each has 47 syllables, making the polyalphabetic tableau a gigantic one of 2,209 cells, more than three times as extensive as the ordinary Vigenere tableau of 676 cells.

Nevertheless, by about 5:30 the next morning he had a

solution. His inability to apply symmetry of position to the unrelated alphabets gave it a certain amount of slack, but he regarded it as essentially sound. He showed it to Rochefort. That expert noted the weak spots and said to Wright in mock rebuke:

"I can't send this out."

"If you don't," Wright replied firmly, "I will."

Rochefort laughed. He had only been testing Wright's faith in the solution, and Wright knew it. "Go ahead," he said.

Wright took it up to communications for transmission via the secret channel to the other communications intelligence units. He then headed once again for home, and on the way saw Layton about 7:45 and told him about it. Within hours, Nimitz knew that the Japanese had ordered that the Midway operation was to commence June 2 against the Aleutians and June 3 against the atoll. His intelligence staff had forecast correctly—but what a relief it was to know for sure, to work on fact instead of on theory.

By this time—the middle of the week before the attack was due—*Enterprise* and *Hornet* had reached Pearl after racing up from the southwest. *Yorktown* limped in the next day, her bowels torn by a Coral Sea bomb. Peacetime structural repairs would have taken 90 days; now the Navy yard, goaded by Nimitz, who knew how soon the hammer would fall, did the impossible and patched her up in two. On the 27th, Nimitz had issued his Operation Plan 29-42, stating that "The enemy is expected to attempt the capture of Midway in the near future" and setting forth his dispositions for the counterattack. He ordered his carriers to a position codenamed POINT LUCK about 350 miles northeast of Midway. Here, on Yamamoto's flank, where they were not likely to be scouted, they were to await his advance. Then, with the advantage of the surprise that the American cryptanalysts had wrestled from the unsuspecting Yama-moto, they were to spring on him, repulse the Midway invasion, wreak havoc on his carriers, and finally cheat him of the naval victory on which his war-winning strategy depended.

The three carriers took up station at POINT LUCK on June 2. By then the Japanese had succeeded in effecting their long-desired code change. It completely blacked-out • the cryptanalysts of the Combat Intelligence Unit. They began chipping away at what they called jN25c, but they

I

got only a few glimmers of light before edition d came into force, unexpectedly soon, in August. Had the June change been made in April as the Japanese had originally wanted, the cryptanalysts, Dyer said, "could not have gotten back in in time to do any good. May 1st would have been impossible. Midway was therefore a very close thing." But the June change did not affect the course of events, since all plans had been made and the great operation had already been set in motion.

According to program, the Japanese Aleutian force struck first. Nimitz had sent a North Pacific Force of cruisers and destroyers to protect his flank. Like some other officers, its commander, Rear Admiral Robert A. Theobald, suspected that the Japanese had "planted" the information on which U.S. intelligence estimates were based. They were probably thinking of dummy radio activity to fool the traffic analysts, for Nimitz never mentioned the supersecret cryptanalytic successes to his force commanders—not even in the briefings just before the battle. The suspicions of the doubters may have been reinforced by an intercepted plaintext request of a Japanese Army officer that all mail for his unit be addressed to Midway after June 5; as General Marshall later said, "that seemed a little bit too thick." Furthermore, Nimitz himself warned of Japanese trickery when arranging for identification by radio in his Operation Plan 29-42: "The Japanese are adept at the practice of deception. Have authenticators ready for use when needed. Small craft and aircraft except patrol planes use two alternate letters from the expression: 'Farmer in the dell.' Example: RE or EL or NH." Hence Theobald disbelieved the intelligence supplied him that the Japanese were going just to bombard Dutch Harbor but to seize Attu and Kiska. He deployed his force to prevent what he was convinced would be an invasion of Dutch Harbor. Unfortunately, this disposition deprived him of any opportunity to fight when, on the morning of June 3, right on schedule, the Japanese did just what the cryptanalysts had said they would do and bombed Dutch Harbor, inflicting considerable damage. They escaped unmolested.

The same morning an American search plane from Midway spotted the enemy. It was the troop-carrying invasion force, which Midway-based planes promptly but ineffectually attacked. The main striking force of four big carriers—*Akagi, Kaga, Hiryu,* and *Soryu,* veterans of the

Pearl Harbor attack—remained hidden by clouds until the next morning, June 4. Again a Midway scout discovered the vessels. The American carriers sped toward them to launch planes for an attack. Meanwhile, American bombers from Midway and Japanese bombers from the carriers were mounting simultaneous attacks. Neither did much damage. Returning Japanese planes told of the need for further attacks.

So far the Japanese had sighted no American ships. They had not been diligently looking for them because, according to their expectations, no major enemy forces should have been in the vicinity: they should have been in Pearl, waiting to find out where the Japanese would strike. Admiral Chuichi Nagumo therefore struck below the 93 planes he had prudently held to counter even the highly unlikely enemy naval attack and ordered them rearmed for land bombardment. Thirteen minutes later he was dumbfounded to receive a report of the sighting of enemy ships to the northeast. What should he do? For a precious quarter of an hour he mulled it over. Finally he canceled his order and directed the planes readied to attack ships. The incendiary and fragmentation bombs that the crews had just sweated into the bomb bays had to be replaced with the original torpedoes and armor-piercing bombs. Before this work was completed, his airplanes began returning from Midway, and his carriers had to recover these before launching the others.

It was at this most vulnerable of m ments—with all planes aboard, with fueling in process and bombs and ammunition stacked in the open on the hangar and flight decks —that American planes attacked. Three waves of torpedo-bombers, one each from *Hornet, Enterprise,* and *Yorktown,* swept in, suffered heavy losses under Zero attacks or antiaircraft fire, and scored not a single hit. The last plane zoomed away at 10:24 a.m. This moment marked the high tide of Japan's fortunes in World War II. Jubilant officers cheered what they thought was victory at Midway, and in the war. Within six minutes, the tide was ebbing.

Dive-bombers from *Enterprise* screamed down on *Akagi, Kaga,* and *Soryu.* One hit set off *Akagi's* torpedo storage, another exploded amid planes being rearmed on her flight deck; flames swept her, and within 24 hours she had been sunk. *Kaga* took four hits in rapid succession and sank that evening. *Yorktown* dive-bombers pummeled *Soryu*

with three half-ton bombs; within 20 minutes she had to be abandoned, and a few hours later was torpedoed by an American submarine. The work of December 7 had not been completed, but avenged.

The rest was anticlimax. Later in the day *Hiryu* was sunk, and the Japanese in turn got *Yorktown.* Yamamoto next day realized that he was beaten. He called off the invasion of Midway and retreated, keeping close to his cabin on the homeward voyage. The samurai chieftains canceled plans for further advances and shifted from offense to defense. The failure to destroy the American Navy knocked the keystone from Yamamoto's strategy, and his words to Prince Konoye before the war haunted him: "I must also tell you that, should the war be prolonged for two or three years, I have no confidence in our ultimate victory." And not only did American industrial strength rise up like a specter. Japan's lack of it meant that she would never recover from the loss of four big carriers. The 4th of June had doomed her.

"Midway was essentially a victory of intelligence," Nimitz has written. "In attempting surprise, the Japanese were themselves surprised." General Marshall was even more specific. As a result of cryptanalysis, he declared, "We were able to concentrate our limited forces to meet their naval advance on Midway when otherwise we almost certainly would have been some 3,000 miles out of place." The surprise, the concentration, were engineered days before in a basement office a thousand miles from the scene of the action, where the solution of messages in JN25b (abetted by the recoveries of the other cryptanalytic units) and its internal time and place ciphers forged effects more crucial to the course of history than any other solution except that of the Zimmermann telegram. The codebreakers of the Combat Intelligence Unit had engrossed the fate of a nation. They had determined the destinies of ships and men. They had turned the tide of a war. They had caused a Rising Sun to start to set.

There was no single moment when the Battle of Midway was suddenly and decisively won, and so there was no burst of wild cheering in the basement office. The cryptanalysts reacted prosaically. The unit went on a watch in three instead of a watch and watch. It was also expanding rapidly. By the next year, it had changed its name to Fleet Radio

ini-N i/vi^a

Unit, Pacific Fleet—FRUPAC, in the Navy's interminable list of acronyms. Rochefort had departed in October, 1942, for two years of noncryptologic duties. He was replaced by Captain William B. Goggins, 44, a 1919 Annapolis graduate with long communications experience. Goggins, who had been wounded in the Battle of the Java Sea, remained as head of FRUPAC to January, 1945. Dyer continued to head cryptanalysis. Eventually FRUPAC comprised a personnel of more than 1,000. Much of the work was done in the new Joint Intelligence Center, housed in a long narrow building across Midway Drive from Nimitz' headquarters perched atop a cliff overlooking Pearl Harbor. Fabian, in Melbourne, directed a field unit similar to FRUPAC. He was on the staff of the Commander in Chief, 7th Fleet, which was attached to MacArthur's South West Pacific Area command.

FRUPAC'S growth mirrored that of all American crypt-analytic agencies. This expansion compelled OP-20-o to reorganize as early as February, 1942. The workload had become too heavy for one man (Safford). The outfit was split up into sections for its three major cryptologic functions : (1) the development, production, and distribution of naval cryptosystems, headed by Safford; (2) policing of American naval communications to correct and prevent security violations; (3) cryptanalysis, headed by Commander John Redman. In September the development function was separated from the production. Safford retained control of the development work until the end of the war, devising such new devices as call-sign cipher machines, adapters for British and other cryptographic devices, and off-line equipment for automatic operation. About June, the Navy ceded Japanese diplomatic solutions to the Army, giving over its files as well as its PURPLE machine. So rapidly was the workload expanding, however, that this diminution of its responsibility did not prevent the cryptologic branch from bursting the seams of its Navy Department building offices. In 1942, it moved into the brick buildings of a former girls' school at 3801 Nebraska Avenue, at the corner of Massachusetts Avenue, in a quiet section of northwest Washington. In the fall of 1941, about 700 persons, including 80 officers, had been doing communications intelligence in the entire Navy; two thirds of them were intercepting, direction-finding, or training for that work; the others, including most of the officers, were solv-

ing and translating. By the end of the war, there were 6,000.

The Army's growth was even more spectacular. It multiplied its communications-intelligence manpower thirty-fold from its strength December 7, 1941, of 331—44 officers and 137 enlisted men and civilians in Washington, and 150 officers and men in the field. Ever-growing requirements quickly dwarfed early estimates, such as the one early in 1942 that a staff of 460 would suffice, and kept up a relentless pressure for more and still more workers. Yet the agency faced stiff competition for them in manpower-short Washington. Moreover, the necessity for employees to be of unquestionable loyalty and trustworthiness, because of the sensitive nature of cryptanalytic results, and the importance of their being temperamentally suited to the highly specialized nature of the work, greatly reduced the number of prospects. To fill its needs, the agency launched a series of vigorous but discreet recruiting drives. It snatched people out of its school even though they were only partially trained: during the school's entire time at Fort Monmouth, New Jersey, not one student completed the full 48-week course. It brought in members of the Women's Army Corps—almost 1,500 of them. These measures enabled the agency to grow to a strength of 10,609 at its peak on June 1, 1945—5,565 civilians, 4,428 enlisted men and W.A.C.'s and 796 officers. (This figure excludes cryptologic personnel serving under theater commanders overseas.) Nevertheless, the personnel supply never caught up to the demand. In April, 1944, for example, the agency had more than 1,000 civilian positions empty.

But its growth soon made more space necessary. Like the Navy, it found a former girls' school ideal for its purposes. During the summer of 1942, it moved from the Munitions Building to Arlington Hall, whose brick buildings stood on 58 wooded acres fronting on Glebe Road in Arlington, Virginia, about three miles from downtown Washington and away from the eyes of enemy agents. The agency soon outgrew even this, and in the late fall of 1942 began expanding into Vint Hill Farms, an old estate in the Virginia horse country about 50 miles from Washington. Giant intercepting towers and half a dozen ugly barracks-like buildings soon disfigured the lovely Blue Ridge foothills, and here, in rooms filled with desks with tilted tops,

most of the Army's traffic analysis was done. In addition, the agency taught most of its cryptology here, with the removal of its school from Fort Monmouth in October, 1942.

In June of 1942, owing to a reorganization in the Office of the Chief Signal Officer, the outfit shed its old name of Signal Intelligence Service and gained and lost three new ones within two months. Then from July, 1942, to July, 1943, it was called the Signal Security Service, and from July, 1943, to the end of the war, the Signal Security Agency. Lieutenant Colonel Rex Minckler, chief since before Pearl Harbor, was replaced in April, 1942, by Lieutenant Colonel Frank W. Bullock. In February, 1943, Lieutenant Colonel W. Preston (Red) Corderman, tall, husky, quiet, pleasant, who had studied and then taught in the S.I.S. school in the 1930s, became chief. He remained in the post to the end of the war, rising to a brigadier general in June, 1945.

Its population explosion and its voluminous output strained its administrative structure, and this was realigned several times. As of Pearl Harbor it was divided into four sections: the A, or administrative; the B, or cryptanalytic; the c, or cryptographic, and the D, or laboratory.

The c, or cryptographic section, devised hundreds of codes and ciphers during the war and produced thousands of key lists. It printed 5,000,000 classified documents, some running to many pages each, and distributed them in a carefully guarded manner throughout the world, accounting for each one. It tested the security of Army cipher machines (mainly Friedman's M-134 SIGABA) by attempting to solve them—and found that they generally proved impregnable. It supervised the mechanization of Army cryptography—the increasing replacement of strip cipher and M-209s and similar slow systems with typewriter-keyboard cipher machines, often with an on-line capacity. Only such mechanization enabled Army cryptographers to keep up with the ever-rising flood of traffic: the 23,000 codegroups a day that the 5th Army headquarters processed during its Sicily campaign strained even the machines to their limit—and by the time that army was marching on Rome, its headquarters was handling 40,000 groups a day. Traffic volume passed belief: in Hollandia, a million groups a day in November, 1944; at the Army's European Theater of Operations headquarters even before OVERLORD,

1,500,000 to 2,000,000 groups a day, or the equivalent of a shelf of 20 average books. The biggest message center of all, the War Department's in Washington, handled its peak load on August 8, 1945: nearly 9,500,000 words, the equivalent of almost one-tenth the total of French intercepts in all of World War I.

In August of 1942, subsection 6 (traffic) of the crypt-analytic section was upgraded to an E, or communications, section, to disseminate the solutions and to send directives to the field intercept units. In December, the shop of the cryptographic section was set up as the nucleus of the F, or development, section, for cryptographic equipment. In March of 1943, all six sections were elevated to branches, and by the following year two more had been added: the machine and the information and liaison branches. The Army had begun to use machines for cryptology in 1936, when Hollerith tabulating machines facilitated the compiling of codes. Their cryptanalytic potential had also been noted in that same year. By Pearl Harbor, 13 I.B.M. machines tended by 21 operators were working on S.I.S. projects. The personnel-short agency converted as many tasks as possible to mechanical operation, and the o, or machine, branch grew to enormous proportions. The 407 machines and 1,275 operators that it had by the spring of 1945 handled accounting and cryptologic tasks that would otherwise have required the hand labor of impossible numbers of clerks.

The cryptanalytic branch, then headed by Solomon Kull-back, one of the three original cryptanalysts hired by Friedman in 1930, was much the largest, with 2,574 people in July of 1944, 82 per cent working on Japanese Army messages. To balance the agency and reduce the number of branch chiefs reporting to its commanding officer, the agency was reorganized the following month into four divisions: intelligence, which did traffic analysis and crypt-analysis; security, which handled cryptography and radio countermeasures and formulated and executed policy and technical doctrines; operating services, which provided services for the intelligence and security divisions and ran the secret-ink laboratory; and personnel and training.

Though this set-up held until the war ended, operational control of the agency passed on December 15, 1944, to *c-2,* the military intelligence section of the War Department General Staff, which was the agency's major customer and

which, as such, for many months had indirectly guided its activities. The Signal Corps merely retained administrative control. This confusing arrangement—complicated further by the agency's having both staff and command functions— ended in August, 1945, when the War Department transferred all signal intelligence units to agency control. On September 6, four days after the war ended, the War Department ordered the creation within G-2 of a new cryptologic organization by merging the Signal Security Agency, the field cryptanalytic units, and Signal Corps cryptography. This was the Army Security Agency, which came into existence September 15, 1945.

Throughout the war, most of the intercept material for Signal Security Agency headquarters was supplied by the 2nd Signal Service Battalion. It had been created as the 2nd Signal Service Company on January 1, 1939, by Major General Joseph Mauborgne, the chief signal officer, out of the 1st Radio Intelligence Company at Fort Monmouth, plus the radio intelligence detachments of signal companies in the Canal Zone, Fort Sam Houston, Texas, the Presidio, San Francisco, Fort Shafter, Hawaii and Fort McKinley, Philippine Islands. Commanding its 101 enlisted men was First Lieutenant Earle F. Cooke. It grew rapidly—in October, 1939, a detachment under First Lieutenant Robert E. Schukraft arrived at Fort Hunt, Virginia, to install and operate a new Army intercept station. With the onset of war, the imperative demands for manpower compelled the Army, on April 2, 1942, to increase the company to battalion strength. Eventually it expanded to an enormously oversized company of 5,000 men. From April, 1942, to the end of the war, its commanding officer was the Signal Security Agency chief. When G-2 took operational control, the battalion was redesignated the 9420th Technical Service Unit, which at the end of the war became part of the Army Security Agency. By that time, the original four radio circuits on which it was sending intercept material back to Washington at the time of Pearl Harbor had swollen to 46 full-time radioteletypewriter channels.

The Army, like the Navy, established cryptanalytic units in the several theaters of war. Their organization varied from one theater to another. The South West Pacific Area, Under MacArthur, had at its headquarters a communications-intelligence unit called the Central Bureau and in the field a number of subordinate units. Central Bureau, or

I '

l^ll

simply C.B., had been founded in August of 1942 by Lieutenant Colonel Joe R. Sherr, who had been head of the 18-man 2nd Signal Service Company detachment in the Philippines and who had accompanied MacArthur to Australia. Later, Abraham Sinkov, who had been another of Friedman's original cryptanalysts, went out to take charge. C.B. was quartered in a rambling wooden house—which local legend said was a former whorehouse—close to the Ascot racetrack in Brisbane. A guard stood in front. A small air-conditioned brick building at the track itself housed the I.B.M. machinery. Sinkov worked -wonders: when a downed Japanese bomber yielded an air-to-ground codebook, it was discovered that Sinkov had already recovered nearly all of it. His title at the end of the war was Cryptanalytic Officer, Signal Intelligence Service, U.S. Army Forces, Far East; his rank by then was colonel. A sweet and unmilitary man who seemed slightly embarrassed by the eagles on his shoulders, he was unable to return a salute without blurting out a "Good morning." He was awarded a Legion of Merit and an Oak Leaf Cluster to it for his work.

Some elements of the Central Bureau were—despite the name—attached to widely scattered units. MacArthur's chief signal officer, Brigadier General Spencer B. Akin, who enjoyed more authority than any other theater signal officer, attached communications-intelligence units to major headquarters so that the intelligence would be promptly available to officers who could act upon it. He even assigned one such detachment to Admiral William F. Halsey, Jr.'s flagship, while Admiral Spruance found the Army service so valuable, when he took command of the 5th Fleet, that he kept the communications-intelligence specialists with him.

In addition, Signal Corps radio intelligence companies provided tactical, combat-level communications intelligence, One of the first, the 101st Signal Company (Radio Intelligence), replaced Hawaii's old Monitor Post 5 in July of 1942, vastly improving the quantity and quality of the work. Typical, perhaps, of these companies was the 138th. Trained in Spokane for Europe and then transported to the East Coast, it was loaded aboard a transport and promptly shipped through the Panama Canal to Australia, landing there in June of 1943. The 299-man company was mobile and self-contained so that it could operate in isolation: it

was mountable within two hours and had its own truck-drivers, cooks, repairmen, and so forth. The men lived in tents.

The company's mission was to determine the Japanese order of battle and ascertain military concentrations and movements. Most of its work involved air-to-ground messages. To pick up these low-power transmissions, it had to move forward from island to island as the Allies advanced. Its first position, early in 1944, was at Nadzab, an airstrip in the Markham Valley of New Guinea. One subordinate direction-finding group was over a hump at Gusap; another was on an abandoned ranch near Darwin, Australia, where it enjoyed fresh meat daily. In the middle of the year it advanced to Biak, a small island north of New Guinea, where it was nearly strangled by the thick jungle, and it went ashore on Leyte about five days after the first wave of invasion troops. By then its direction-finding groups were scattered all over the South Pacific.

The unit worked near the front lines so as to get as many intercepts as possible. So close were they that on Leyte late in 1944 Japanese paratroops dropped on the unit, apparently having mistaken it for a command post because of its numerous antennae. One startled radioman, isolated in a direction-finding booth in the middle of a clearing, suddenly heard bullets whizzing all around him. The codebreakers dropped their pencils, grabbed their rifles, and engaged in rather more direct action against the enemy than that to which they were accustomed. The paratroopers were driven off, but not quickly enough to save the unit's documents from the flames.

Its radio operators, specially trained in Japanese Morse, listened in 24 hours a day on at least some of its two dozen receivers. Sometimes just the circuits being used would give Japanese intentions away. On Biak in 1944, the unit quickly learned that messages on a certain frequency invariably preceded an evening air raid—a bit of foreknowledge that enabled one member to collect regularly on sure-fire bets with a sergeant from a nearby outfit. Other times the 20-odd nisei in the unit intercepted Japanese cleartext. Usually, however, the radiomen typed out the coded intercepts and handed them to a traffic analyst. Most of the messages reported planes flying from one point to another, and the analyst, by a study of call-signs, could tell which unit and which points were meant. The 15

cryptanalysts had the mechanical task of stripping the additive from codes that had been solved at C.B. Each day a report summing up the unit's conclusions went rearward to 5th Air Force headquarters, to which the unit had been attached, switching from the Signal Corps under C.B. to the Army Ah* Corps and receiving the new name of 1st Radio Squadron, Mobile.

Success usually came in the humble form of an early warning of an air raid that probably saved American lives, or as some insight into a Japanese move that enabled an American commander to neutralize it. Late in the war, the unit's solution of Japanese meteorological codes told American bombing commands what they wanted to know most —weather conditions over target. The outfit alerted the Allies to a major Japanese build-up when it solved a message reporting the presence in an airplane of two high-ranking officers of Japan's 4th Air Army, which up to that time had been thought to be in northern China. But its greatest feat was the discovery of a huge concentration of Japanese air strength in Hollandia. The 5th Air Force launched massive raids and destroyed more than 100 enemy planes. Consequently they were not present to attack the American invaders, who splashed ashore with virtually no opposition.

The Imperial Japanese Navy had commenced its crypt-analytic efforts in 1925 with the creation of an ultra-secret Tokumu Han ("Special Section") in the 4th, or communications, Department of the Naval General Staff. It then numbered six persons, including clerks, and was located in the red brick Navy Ministry building in Tokyo. Among its early members were the young naval officer Hideya Morikawa, nephew of Chief of Staff Admiral Kanji Kato, and Morikawa's former superior, First Lieutenant Kamisugi, who had handled cryptography aboard the flagship *Nagato.* Captain Kowalefsky, the Polish cryptologist who had improved the codes that Yardley had solved, lectured on cryptanalysis, and the neophyte codebreakers cut their eyeteeth on the GRAY code of the U.S. Department of State, making their entry through the classic technique of identifying NADED as *period.**

*Whether this solution was made in cooperation or in competition with the Ango Kenkyu Han, the Foreign Ministry's cryptanalytic section, is not known.

They also solved Chinese cryptograms during the Manchuria incident, primarily because these were based on a commercial codebook that transformed the Chinese ideographs to four-digit numbers for telegraphic communication. After the Japanese seizure of Shanghai early in 1932, Morikawa was sent there as chief of a cryptanalytic unit attached to the 3rd Fleet. He solved a Chinese message that corroborated a slightly doubtful Tokumu Han solution of an American GRAY message reporting Chinese plans to use its Air Force to attack Japanese troops. Instead the Japanese struck first, catching most of Chiang Kai-shek's Air Force at Hangchow.

The Tokumu Han failed, however, to break two-part codes, such as the State Department's BROWN code, those used by the American Navy, and those introduced by Yardley into Chinese communications when he was Chiang's cryptologist—except in extraordinarily favorable circumstances. One such occurred on February 26, 1936, when two regiments mutinied in Tokyo and several statesmen were assassinated in an attempted coup d'etat. This furnished the cryptanalysts with an ocean of text and plenty of probable words to go fishing with. For a short time they read most American communications, including those of the naval attache. Then the United States changed systems, and the skill of the Tokumu Han again proved unequal to its task. Its resourcefulness made up for this: near the end of 1937, Morikawa, accompanied by a locksmith, a photographer, and some lookouts, broke into the American consulate at Kobe and photographed the BROWN code and the M-138 cipher device, which the Japanese had never seen before.

Soon thereafter, as part of Japan's preparation for war, the naval shoguns built their first big intercepting post at Owada, a village about fifty minutes by car from Tokyo. During American naval maneuvers, its direction-finding and traffic analysis helped the general staff analyze American forces and tactics. The Tokumu Han also added crypt-analysts, all of whom were officers. By Pearl Harbor there Were ten working full time and ten part time. They had still not succeeded, however, in reading American cryptograms.

After Pearl Harbor, the rampant growth of Allied communications compelled the Tokumu Han to expand still further. The first batch of recruits—60 of them—were

drawn form foreign-language schools and commercial colleges to become the first civilians in the Tokumu Han. The second batch consisted of about 70 reserve officer candidates selected from about 500 in basic training on the basis of their competence in foreign languages. (These signal intelligence groups differed from classes learning cryptography.) During a five-month course at the Naval Communication School at Kurihama near Yokosuka— hard by the Commodore Matthew Perry monument—they practiced International Morse, studied the elementary Oriental Tenji and Tenchi ciphers as well as the Occident's more advanced Porta and Vigenere, and learned how to break codes and ciphers. Six classes, each larger than its predecessor, were trained during the war. Some graduates were assigned to communications intelligence in the intelligence units of fleet and force headquarters. In November of 1943, for example, the 3rd Fleet employed three officers and six enlisted men to monitor enemy messages. But most went straight into the Tokumu Han proper.

A torrent of intercepts was pouring into it. Most came from the hundreds of radio receivers and direction-finders of the Owada Communications Unit. Some were picke up by the 20 Americans and Australians pressed into sei vice with the Kanagawa Communication Force nea Hiyoshi, and a few messages trickled in from fleet radi units. Near the end of the war a unit was set up in radish field at Yokosuka. The entire Tokumu Han ha swollen to several thousand men by the end of the wai most engaged in intercepting. So hungry was it for competent personnel that it did something almost unheard-of in misogynistic Japan; it employed women—putting about 30 nisei girls to work eavesdropping on American radiotelephone conversations. By the middle of 1943 it had outgrown its quarters, and the traffic analysis section moved to the third floor of the Naval War College in Tokyo, leaving only the cryptanalysts at the Navy Ministry.

They comprised the 2nd Branch of the Tokumu Han's three. In charge was Captain Endo. Under him were several national sections: United States and Britain, with about 50 officers under Lieutenant Commander T. Satake; China, with about 20 officers under Lieutenant Commander Nakatani; Russia under Lieutenant Commander Masayoshi Funoto; and Italian, German, French, and others, about 10 officers. The 3rd Branch handled traffic analysis. It was

J

likewise organized on a national basis, subdivided into areas, with an average of two officers and a handful of enlisted men working on each area. This was fluid, however, and sometimes as many as ten officers would be working on a single area. The branch was commanded by Morikawa, now a captain, who, in a separate capacity, also headed the Owada Communications Unit. The 1st Branch planned, made policy, and distributed the results of the two operating branches. In charge was Captain Amano, with Commander Hideo Ozawa his executive officer. Command of the entire Tokumu Han was vested in the chief of its parent body, the 4th Department; in effect, this gave the Tokumu Han a seat on the Naval General Staff. In 1943 the head of the 4th Department was Rear Admiral Gonichiro Kakimoto, and at the end of the war, Rear Admiral Tomekichi Nomura.

In sharp distinction to American cryptanalysts, who were reading the vast majority of Japanese messages, including those in the cryptosystems of topmost security, the code-breakers of the Tokumu Han failed almost completely in extracting usable information from American messages. They did not even attempt to solve medium- and high-echelon messages, couched in cryptosystems far beyond their ability. They concentrated instead on three simpler cryptosystems of the lowest level of command. Even with these, they achieved only limited success.

Typical was their experience with a small code that they called AN 103. Carried by U.S. Navy patrol planes, it consisted of a few dozen expressions, such as *enemy sighted.* The code was changed every seven to ten days, but the same plaintext expressions appeared in successive editions, facilitating solution. Fortunately, such solutions were usually obtained too late to take any action based on them.

The Tokumu Han cryptanalysts succeeded best with BAMS, the two-part superenciphered Allied merchant ship code. They solved about half of the BAMS intercepts. How Were they suddenly able to do so well with so relatively difficult a system? Germany had given them the basic BAMS codebook, which had been captured by her raider *Atlantis.* Consequently, the Japanese had only to remove the superencipherment. BAMS provided occasional tidbits pf information—three transports had departed from Cal-tfornia, for example, or a vessel's course and speed data— out even here, Ozawa complained, "By the time the code

[message] was broken, the ship was no longer in the original area."

The Tokumu Han expended most of its cryptanalytical energies on the CSP 642, the strip cipher, which the U.S. Navy regarded as its lowest-echelon system. The Navy complicated it by not using the full complement of 30 strips every time. Instead it eliminated from zero to five strips from one day to another. Thus one day's messages might use only 25 strips, the next day's, 27, the next, 30.

Japan had captured strip ciphers on Wake and Kiska, and with these she attacked the intercepts. Her methods mixed sophistication and naivete. To determine how many strips had been eliminated, the Tokumu Han used I.B.M. tabulators of the First Life and the Maiji Life Insurance companies of Tokyo. These took frequency counts at intervals of 30, 29, 28, . . ., 25 and compared them; the interval that showed the most repetitions indicated the correct encipherment length. Many of the strip messages were sent by American submarines; these were identifiable by their indicators—BIMEC or FEMYH—and by their transmission from close to the Japanese coast. The Tokumu Han could know that at that position a merchant ship had been sunk, or that certain units of the Japanese fleet near there were steaming at such-and-such a course and speed, and that the submarine was reporting this. With this as a lead, two first lieutenants who had majored in English in college, Shimizu and Oda, composed what they thought the plaintext intercept was. They varied expressions, word positions, guesses of latitude and longitude until they had a supposed plaintext that matched the cryptogram in length and whose letters all differed from their ciphertexts— since in the strip system no letter can represent itself. Then they arranged and rearranged the strips until they had reproduced the ciphertext on one line and the presumed plaintext on another; the sequence of strips almost certainly represented that day's key. With it they decrypted other intercepts.

This tortuous method—for some reason they failed to heed the writings of foreign cryptanalysts on solving this system—suggests why so little information was extracted from the strip cipher. The Tokumu Han kept increasing the size of the section in its American branch that handled strip messages until there were about 40 officers, 10 enlisted men, a dozen typists, two dozen women clerks,

Professor Yamanashi of the Navy War College, and a mathematician, Ozaki. Though efforts were continued up to the end of the war, the life had long since gone out of them; the Tokumu Han, considering the strip cipher unbreakable for all intents and purposes, vacated its hopes for crypt-analysis and looked instead to traffic analysis as its chief source of information.

The difficulty with this, as Lieutenant Commander Satake put it, was that "Our whole analysis was based on probabilities; there was nothing of a definite nature." The 3rd Branch graphed the volumes of urgent, priority, routine, and deferred messages transmitted from each major American station. It charted the traffic flow among the various call-signs. It located the transmitters by a widespread direction-finder net of a dozen linked stations situated from Kiska to Rabaul, from Wake to Manila. By following the bulge in BAMS transmissions from California to Hawaii to, say, Guam, the traffic analysts could predict the general area in which the next American assault would come. Messages from reconnoitering submarines or airplanes reinforced the estimate. The time of the attack was often gauged by noncommunications means—such as guesses based on previous movements—but sometimes by such communications intelligence as the imposition of radio silence or an increase in the urgency of reconnaissance messages. None of these methods, however, enabled the 3rd Branch to pinpoint time or place. The Japanese knew in advance, for example, that the United States was mounting an invasion of the Philippines, but when it would come they could tell no more closely than within a month, and upon which island the assault would fall, they never knew until it happened. Compared to the crystalline precision of America's Midway intelligence, Japanese intelligence floundered in a miasma of vaporous generalities. Only once in four years of war—at the Marshalls—did it get word to a garrison early enough to help it prepare for an impending attack.

The Japanese Army, personified by the combined War and Prime Minister General Hideki Tojo, had panted for this war much more than the Navy, and so might have been expected to produce striking communications-intelligence results when the desired hostilities broke out. The woeful actuality was summed up in one sentence after the defeat

or iNippon by Lieutenant General Seizo Arisue, chief of Army intelligence: "We couldn't break your codes at all."

An incident of 1943 epitomizes Japanese incompetence in this whole field. It involved a future President of the United States, who, with his crew, formed the subject of a series of dispatches the Japanese apparently never solved.

These messages were transmitted by three brave Australian coastwatchers, part of a widespread network whose members observed enemy activity from the peaks and cliffs of enemy-held islands, collected tidbits from native allies, and radioed their information to Allied military commands. They frequently gave valuable early warning of Japanese bombing raids and ship movements, and they assisted in the rescue of downed Allied airmen.

In the early morning hours of August 2, 1943, coast-watcher Lieutenant Arthur Reginald Evans of the Royal Australian Naval Volunteer Reserve saw a pinpoint of flame on the dark waters of Blackett Strait from his jungle ridge on Kolombangara Island, one of the Solomons. He did not know then that the Japanese destroyer *Amagiri* had rammed and sliced in half an American patrol torpedo boat, *PT 109,* Lieutenant John F. Kennedy, United States Naval Reserve, commanding. But at 9:30 that morning he received a 20-group message enciphered in Playfair, the coastwatchers' cipher system. He deciphered it with key ROYAL NEW ZEALAND NAVY and learned, *PT boat one owe nine lost in action in Blackett Strait two miles SW Meresu Cove X Crew of twelve X Request any information X.* He reported back to the coastwatcher near Munda, whose call-sign was PWD, that *Object still floating between Meresu and Gizo,* and at 1:12 p.m. he was told by the coastwatcher station KEN on Guadalcanal that there was a possibility of *survivors landing either Vangavanga or islands.*

This was just what Kennedy and his crew had done. They had swum to Plum Pudding Island, one of a group that hangs from the southeastern tip of Gizo Island. This group was behind enemy lines, and Gizo itself, only three or four miles away, was garrisoned by Japanese troops. Though messages about the missing crew continued to stream for the rest of the week between PWD, KEN, and GSE, as Evans called his station (after his wife, Gertrude Slaney Evans), the Japanese made no attempt to capture them.

[Codebreakers 329.jpg]

*Arthur Evans' decipherment of the message of 9:30 a.m., August 2, 1943, that reported the sinking of John F. Kennedy's PT109*

Yet the importance of the crew should have been obvious to the Japanese from the many messages concerning it and from the search mission flown by P-40s, and a capture could not have caused them too much trouble, since on one occasion a Japanese barge chugged right past the island hideout of Kennedy and his crew. Even if they had been intercepting and reading the cryptograms, however, the Japanese may not have wanted to waste time looking for the Americans, since none of the messages specified their location.

This excuse vanished at 9:20 a.m. Saturday morning, August 7. Two natives had found the sailors, who had moved to Gross Island, and had reported the find to Evans. He wrote a brief message: *Eleven survivors PT boat on Gross Is X Have sent food and letter advising senior come here without delay X Warn aviation of canoes crossing Ferguson RE.* He drew up a square based on the current key of PHYSICAL EXAMINATION,

P H Y S I
C A L E X
M N T O B
D F G K Q
R U V W Z

and enciphered the message, departing from traditional Playfair only by leaving doubled letters unenciphered, as the *s's* in *Gross* and *crossing:*
XELWA OHWUW YZMWI

HOMNE OBTFW MSSP1 AJLUO EAONG OOFCM FEXTT CWCFZ YIPTF EOBHM WEMOC SAWCZ SNYNW MGXEL HEZCU FNZYL NSBTB DANFK OPEWM SSHBK GCWFV EK.MUE. A message of

this length would alone suffice for the solution of a Play-fair, and there were four others in the same key, including one of 335 letters, beginning XYAWO GAOOA GPEMO HPQCW

JPNLG RPIXL TXLOA NNYCS YXBOY MNBIN YOBTY QYNAI . . .,

for *Lieut Kennedy considers it advisable that he pilot PT boat tonight X . . . .*

These five messages detailed the rescue arrangements, which offered the Japanese a chance to get not only the shipwrecked crew but the force coming out to save it. All of them could have been solved within an hour by even a moderately experienced cryptanalyst. Yet at 10 p.m. the operation went off without the least hint of enemy interference. It seems likely that had the Japanese solved these elementary enciphered messages, they would have taken some action against the rescuers or the rescued or both. They did nothing. If their communications intelligence had been better, how might contemporary history have been changed!

Their failure sharpens the contrast with Allied successes. For Allied cryptanalysts—which in the Pacific meant mostly Americans—galloped like Tartars through the phalanxed ranks of a legion of Japanese cryptosystems. They ravaged and plundered with a prodigality that did not trifle with petty matters. One system, when solved, proved to be used by direction-finding teams; though this might have afforded some indirect clues to Japanese attacks, it was cast aside for richer treasure. Commander Dyer estimated that American cryptanalysts demolished 75 Japanese naval codes during the war.

Among them was the four-digit code used by the marus, or Japanese merchant vessels—the s code. Presumably this was attacked after the more important combat codes had been resolved. From about 1943, it yielded information of the greatest value: the routes, timetables, and destinations of Japanese convoys. Japan's conquests consisted almost entirely of islands which could be supplied and reinforced only by sea, and Nippon itself was an island empire.

American submarines therefore undertook in the Pacific what U-boats were attempting in the Atlantic, and, as with the U-boats, cryptanalysis helped them achieve their greatest successes.
il

A direct line led from FRUPAC to the office of Captain R. G. Voge, operations officer of the Commander, Submarines Pacific Fleet. The Japanese convoys radioed the positions where they estimated they would be as of noon on the next few days. This was to inform their own forces of their locations, but FRUPAC solved the messages, and Jasper Holmes, an ex-submariner himself, relayed them to Voge, who broadcast them to the American submarines. This fattened their kill. Vice Admiral Charles A. Lockwood, Jr., who was COMSUBPAC during most of the war, estimated that cryptanalytic information stepped up American sinkings by about one third on the trade routes to the Philippines and the Marianas. Eventually the submarine commanders received it so regularly that they complained if a convoy reached its noon position half an hour late!

The pigboats accounted for nearly two thirds of Japanese merchant tonnage sunk during the war. Their torpedoing of 110 tankers from the East Indies resulted in oil shortages in the homeland that prevented the training of badly needed pilots and forced a split-up of Japan's Navy, with serious tactical results. Starvation at home caused Japan to make surrender overtures even before the islands were invaded, before the atom bombs exploded. After the war, Tojo said that the destruction of the merchant marine was one of the three factors that defeated Japan, the others being leapfrog strategy and fast carrier operations. This is why Dyer, looking back, regarded FRUPAC'S solution of the maru code as one of its primary contributions to victory.

American cryptanalysts scored some long-range combat triumphs as well. Shortly after MacArthur invaded Leyte, they discovered from their reading of coded enemy messages that 40,000 soldiers were on their way to reinforce Japanese troops in the Philippines. American air and sea power met and destroyed this force, and not a man reached Leyte. During the Okinawa campaign, the sharp ears of the cryptanalysts overheard the orders that directed the superbattleship *Yamato,* a 72,000-ton monster with 18-inch guns that could hurl a projectile 22 miles, to sortie in a last-ditch defense effort. They passed this news to the American commanders on the spot. Thus alerted, the com-

manders prepared to attack her, and after a picket submarine reported her position, flung wave after wave of carrier-based planes at her. They struck her at 12:32 p.m. April 7, 1945, and after less than two hours of repeated bomb-hits and torpedoings, the world's largest battleship slid to the bottom, rumbling and exploding, and taking with her 2,488 officers and men of her complement of 2,767.

FRUPAC also engendered what is probably the most spectacular single incident ever to result from crypt-analysis.

In the spring of 1943, Admiral Isoroku Yamamoto came down to Rabaul to take personal charge of the deteriorating situation in the Solomon Islands. Japan had just been pushed off Guadalcanal and her supply lines were being snarled by Allied air attacks. Yamamoto welded together the biggest Japanese air armada of the war and sent it against the Allies, achieving some tactical successes. In preparation for further aerial offensives, the stocky, black-browed seaman decided to make a one-day morale and inspection tour of bases in the upper Solomons. Those bases would have to be alerted, together with several other units, so that they could make the many preparations needed for an inspection by the Commander in Chief Combined Fleet. At 5:55 p.m. on April 13, 1943, the commander of the 8th Fleet broadcast Yamamoto's itinerary of five days hence to the 1st Base Force, the 26th Air Flotilla, all commanding officers of the llth Air Flotilla, the commander of the 958th Air Unit, and the chief of the Ballale Defense Unit. The great variety of addressees, plus the need to safeguard the person of the head of the Navy, makes it almost certain that the Japanese communicator selected the current edition of JN25—the most widely distributed high-security code—in which to armor this information.

Unfortunately for the Japanese, this armor plating had been dissolved in the acid of Allied cryptanalysis. As with the pre-Midway solution, the scattered codebreaking units had exchanged their results—possibly augmenting them this time with documents salvaged a few weeks previously from the grounded submarine *1-1.* Though the additive had been changed only two weeks before, on April 1, large portions of it had been recovered. At FRUPAC, these results had been punched onto cards for the I.B.M. machines. FRUPAC'S monitors had intercepted the messages that the 8th Fleet commander had spread on the airwaves, and

when this was fed to the robot cryptanalyst in a form palatable to it, it swallowed it, digested it to the accompaniment of horrendous clickings and rattlings, and disgorged the Japanese plaintext.

Because of the many addressees, the "scanners," or traffic analysts, had probably flagged the message as one of more than ordinary importance. Hence the plaintext went to a translator of more than ordinary competence, a 38-year-old Marine Corps lieutenant colonel, Alva Bryan Lasswell. He had studied Japanese as a language officer in Tokyo from 1935 to 1938 and had helped with communications-intelligence activities in Hawaii since May, 1941. The message was essentially complete, but he helped fill in some holes, while Dyer recovered some additives and Wright determined the meaning of internal geographical codegroups: RR for *Rabaul;* RXZ for *Ballale,* a small island in the Solomons group, just south of Bougainville; RXE for *Shortland,* another of the Solomons, also south of Bougainville and west of Ballale; and RXP for *Buin,* a base on the southern tip of Bougainville. When this work was completed, Lasswell translated the message.

> The Commander in Chief Combined Fleet will inspect Ballale, Shortland, and Buin in accordance with the following:
>
> 1. 0600 depart Rabaul on board medium attack plane (escorted by 6 fighters); 0800 arrive Ballale. Immediately depart for Shortland on board subchaser (1st Base Force to ready one boat), arriving at 0840. Depart Shortland 0945 aboard said subchaser, arriving Ballale at 1030. (For transportation purposes, have ready an assault boat at Shortland and a motor launch at Ballale.) 1100 depart Ballale on board medium attack plane, arriving Buin at 1110. Lunch at 1st Base Force Headquarters (Senior Staff Officer of Air Flotilla 26 to be present). 1400 depart Buin aboard medium attack plane; arrive Rabaul at 1540.
>
> 2. Inspection Procedures: After being briefed on present status, the troops (patients at 1st Base Force Hospital) will be visited. However, there will be no interruptions in the routine duties of the day.
>
> 3. Uniforms will be the uniform for the day except that the commanding officers of the various units will be in combat attire with decorations.

4. In the event of inclement weather, the tour will be postponed one day.

Yamamoto was known to be almost compulsively punctual. He adhered to his schedules virtually to the split second. And Lasswell was now reading almost a minute-by-minute listing of his activities on a day during which the admiral would come closer to the combat zone than he had probably ever done before! The cryptanalyzed intercept amounted to a death warrant for the highest enemy commander.

The question was: Should it be executed? It was not an easy one to answer. Nimitz wrestled with the pros and cons. If Yamamoto were shot down, would a better man be appointed to succeed him? Commander Layton, the fleet intelligence officer, set out the arguments, most of which Nimitz well knew.

Yamamoto, 59, was the dominant figure of the Japanese Navy. A prophet of air power, aggressive and determined, he devised bold, imaginative plans and executed them under strong leadership. He was the Shogi (Japanese chess) champion of his navy, and in the 1920s had enjoyed matching wits with Americans at poker, which he played very well indeed. He has lost two fingers of his right hand in battle, and he manipulated the cards with the remaining three in so wizardly a manner that he distracted his opponents. American intelligence rated him as "Exceptionally able, forceful, and quick-thinking." His men idolized him. "If, at the start of the Pacific War," wrote Commander Fuchida, leader of the Pearl Harbor attack, "a poll had been taken among Japanese naval officers to determine their choice of the man to lead them as Commander in Chief Combined Fleet, there is little doubt that Admiral Yamamoto would have been selected by an overwhelming majority."

Layton summed up with the observation that Yamamoto was preeminent in all categories, that any successor would be personally and professionally inferior, and, finally, that the death of the Commander in Chief would demoralize the Japanese, who venerate their captains much more than Occidentals do. Nimitz concurred. He realized that the shock of such a leader's death, combined with the elimination of the finest strategist of the enemy war machine, would equal a major American battle victory. He was furthermore

probably influenced by the general American hatred of Yamamoto. Naval officers knew that he had conceived the treacherous strike at Pearl Harbor that had slaughtered their shipmates and wrecked their ships. He had, they thought, arrogantly boasted that he would dictate peace in the White House.* This was why Admiral William F. (Bull) Halsey made him "No. 3 on my private list of public enemies, closely trailing Hirohito and Tojo."

By chance, the Ballale-Shortland-Buin area was in Hal-sey's theater of operations. Consequently Nimitz sent him a top-secret command-level communication referring to the Yamamoto itinerary and authorizing him to shoot down the Japanese planes if his forces had the capability of doing so. Halsey was in Australia; his deputy, Vice Admiral Theodore S. Wilkinson, reported that he could do it, but invited Nimitz' attention to the danger of making the Japanese suspicious that the Allies were reading their codes. If they changed them, might not this deprive the Allies of possibly even more valuable intelligence in the future?

Nimitz felt that this bird in the hand was well worth stay two in the bush. Nevertheless, he sought to minimize the danger by following Layton's suggestion of a cover story. This was to the effect that Australian coastwatchers had radioed in the Yamamoto flight information, probably getting it from friendly natives around Rabaul. The coast-watchers enjoyed a superexcellent reputation among airmen and so the story would ring true. If it got back to the Japanese, they might never even think about codes. Even if they did realize that the Allies were reading their codes, either by capture or by cryptanalysis, they could probably do no more than issue a new edition of JN25 and perhaps tighten cryptographic security. But this had happened before, and Allied cryptanalysts had broken the new codes. The most realistic assessment predicted that the Yamamoto mission might temporarily dim Allied communications intelligence while cryptanalysts sought entry into the new code.

Such a loss of information is never good, but it would be less unfortunate now, when the Allies were resting and consolidating their positions, than during a major opera-

*This was later proved to be a canard, but its authenticity was accepted at the time.

tion. No such advance was planned for two and a half months. Hence if the Japanese changed their code immediately after Yamamoto's death, the cryptanalysts would have ten weeks of relative quiet to break back in. In his reply to Wilkinson, therefore, Nimitz ordered him to brief all personnel on the cover story, iterated his authorization, and added a personal "good luck and good hunting" to the message.

The death warrant was now signed, sealed, and delivered.

On the afternoon of April 17, Major John W. Mitchell and Captain Thomas G. Lanphier, Jr., both of the Army Air Corps, walked into a dank and musty Marine dugout on Henderson Field, Guadalcanal. An operations officer handed them a cablegram on blue tissue—the kind used for top-secret dispatches. It detailed Yamamoto's itinerary, including times of arrival and departure from each place. The airmen vetoed a suggestion to strafe him while crossing from Ballale to Shortland in the subchaser because of the difficulty of identifying the right craft. Instead they decided to intercept him in the air.

Their plan depended upon Yamamoto's punctuality and required careful timing of its own: Ballale was near the limit of range of the twin-engined P-38 Lightnings that the pilots flew, so there would be little fuel for waiting. Though the Japanese message specified arrival at Ballale at 8 a.m. after a two-hour flight from Rabaul, calculations showed that the two-motored Mitsubishi (Betty) attack bombers would reach Ballale in an hour and 45 minutes; this was partially confirmed by the estimated hour-and-40-minute return time from the slightly closer Buin. This meant that Yamamoto would arrive at Ballale about 7:45 a.m. Though he would be escorted by six fighters, Mitchell and Lanphier decided to attack him about 35 miles up the Bougainville coast to avoid the planes that buzzed around Kahili airstrip not far from Buin. This pushed the time of interception back ten minutes to 7:35 a.m.—or 9:35 a.m. American time.

Next morning, 18 P-38s of the 12th, 339th, and 70th Fighter Squadrons lifted off the Henderson runway at 7:25 (American time). Thirty-five minutes later and 700-odd miles away, Yamamoto's flight took off right on schedule. Radios silent, the Americans flew a semicircle of 435 miles around Munda, Rendova, and Shortland at wave-top height

to avoid radar detection. Mitchell navigated by compass and airspeed indicator, and two hours and nine minutes after take-off was skimming the waves toward the Bougainville coast. He had timed the flight to the split second, and suddenly, as if the entire affair had been rehearsed to perfection, the black specks of Yamamoto's squadron appeared five miles away.

"Bogey. Ten o'clock high," called out Lieutenant Doug Canning, breaking radio silence. Mitchell led 14 fighters up to 20,00 feet as cover and to engage the fighters. Lanphier dropped his belly tanks, and, with his wing man, Lieutenant Rex T. Barber, climbed to within two miles of Yamamoto's right and a mile in front of him before his escorting Zeroes saw them and turned to attack. Lanphier disintegrated one of them, then kicked his ship on its back and looked down for the lead bomber. He spotted it dodging away at tree-top level. As he spun toward it, two Zeroes dived at him. But, he said, "I remember suddenly getting very stubborn about making the most of the one good shot I had coming up. I fired a long steady burst across the bomber's course of flight, from approximately right angles. The bomber's right engine, then its right wing, burst into flame. . . . Just as I moved into range of Yamamoto's bomber and its [tail] cannon, the bomber's wing tore off. The bomber plunged into the jungle." The Zeros screamed helplessly overhead. Barber, meanwhile, exploded the other Mitsubishi. Lanphier shook his pursuers in a speedy climb to 20,000 feet, and he and all the other members of the mission except one returned safely to Henderson.

Deep in the Bougainville jungle, Yamamoto's devoted aide found his admiral's charred corpse still in its seat, its chin on a samurai sword. The body was extricated with care and solemnly burned. On May 21 a Japanese newscaster announced, in tones heavy with sorrow, that Yamamoto, "while directing general strategy on the front line in April of this year, engaged in combat with the enemy and met gallant death in a war plane." Toward the end of the communique his voice became choked, as if through tears. As Layton and Nimitz had foreseen, Yamamoto's death stunned the entire nation. On June 5, his ashes were interred with great pomp in Tokyo's Hibiya Park in the presence of the government and an immense and silent crowd. The death of the great popular hero disheartened

Japanese soldiers, sailors, and civilians. "There was only one Yamamoto, and no one is able to replace him," said the man who succeeded him. "His loss is an insupportable blow to us." Cryptanalysis had given America the equivalent of a major victory.

What happened to cryptology during World War II?

The war worked no changes as basic as those of telegraphy, which revolutionized the structure of cryptography, or of radio, which ushered cryptanalysis into the world as a factor of importance. Rather it enlarged, accelerated, intensified what was already there. This held true even in the two most noteworthy cryptologic developments of the war. One was internal, in which the changes were so great as to be qualitative: the evolution in the operations of cryptography and the techniques of cryptanalysis, and one external: the elevation of cryptanalysis from just one among many sources of intelligence to the principal one.

All this resulted, of course, from the immense increase in the use of radio. Blitzkrieg required the closest coordination between motorized spearheads, air support, and consolidating infantry. Global conflict demanded global communications. Unprecedented volumes of traffic streamed through radio channels. To handle it, huge agencies sprang into being.

In World War I, the U.S. Army and Navy had about 400 persons in cryptology (excluding cipher clerks), or about one person in every 10,000 under arms. In World War II, there were 16,000 in cryptology—40 times as many —and the ratio was one person in every 800. In World War I, a handful of officers and enlisted men in the Code Compilation Section had produced codes for the whole A.E.F. In World War II, hundreds of privates at Arlington Hall did nothing but draw up key patterns for the tens of thousands of M-209s all over the world which devoured a new pattern once every eight hours. (Eventually, a linguist on the Hall's think squad devised a mechanism that produced the patterns automatically.) In 1918, a few men had carried the packages of codebooks to the American headquarters that received them. In 1942, Japan was faced with a major logistics task in distributing new code-books to her far-flung forces. Her disastrous pre-Midway failure to do the job in time showed that codes had become cargo almost as essential as food or ammunition. Codes and

ciphers cloaked even more secondary forms of messages—meteorological, direction-finding, airplane, merchant ships'. Intercept stations covered the globe. Branches and subsections sprouted that the science had never known: the Signal Security Service had a special section just to distribute its solutions, another one just to improve and develop cryptographic mechanisms. Brass hats abounded. Recruiting drives were mounted. The whole paraphernalia of large organizations materialized. Cryptology became big business.

At the same time, cryptology completed an evolution in the two core areas of cryptographic operations and crypt-analytic techniques. World War I had left both of them depleted and inadequate. Hand encipherment had barely coped with the message load, even though codes furnished a primitive mechanization. Brute frequency analysis had barely sufficed for the ADFGVX, even though it was handled by a master. The 1920s began to furnish the tools and ideas for which this lack cried out. In cryptography, Vernam, Hebern, Scherbius, Damm, and Hagelin invented practicable cipher machines—secure, portable, rugged, printing. Governments gradually introduced them into service, replacing the old pencil-and-paper methods. In cryptanalysis, Friedman pioneered with statistical methods. Hill opened a window on the new vistas of mathematics. Cryptologic agencies hired mathematicians like Kunze and Kullback and Sinkov as cryptanalysts and purchased tabulating machines to make more calculations. Mathematics generated analytical techniques of great precision and power. These trends, which were still just getting under way in 1939, accelerated with a rush during the war and culminated by 1945. This evolution transformed both cryptography and cryptanalysis and gave each a characteristic it still has. World War II mechanized cryptography and mathematized cryptanalysis.

This development of cryptology's substance, like the growth of its administrative organization, was paralleled by the enormous amplification of its effects. In World War I, cryptanalysis played a central role in one event of high significance—the American declaration of war following the Zimmermann telegram disclosure. In World War II, cryptanalysis helped make possible at least four critical events—Midway, Yamamoto, the rapid cutting of Japan's lifeline, the defeat of the U-boats. Cryptanalysis was not

just a tangential and merely helpful factor; it was a vital one.

•Indeed, the higher in the politico-military realm are the events, the more important becomes cryptanalysis. At the front, it probably stands equal with prisoner-of-war intelligence or aerial reconnaisance. But neither of these can match it for providing insight into the strategic plans of top generals or the basic diplomatic policy of a whole country. A spy may occasionally pluck forth a richer nugget, but he cannot refine the quantity of ore that a cryptanalyst can, nor can he command the credibility. The ungrudging tributes of the two German spymasters attest to this superiority: Walter Schellenberg's acknowledgment that the assistance rendered him by the communications-intelligence chiefs "made most of my success in Secret Service operations possible," and Wilhelm Hottl's boast that his Hungarian cryptanalysts provided him with "at least a hundred successes such as seldom fall to the lot of a Secret Service working in the ordinary ways." General Ame, chief of Italy's Servizio Informazione Militare, listed three succinct reasons why intelligence chiefs like crypt-analysis : it is usually the cheapest, the latest, and the truest source of information.

After the war was over, an American official familiar with the wartime value of codebreaking said that it had shortened World War II by a year. The estimate may be conservative: a Japanese victory at Midway would probably have cost the United States more than a year to come back. When asked about the value of the wartime codebreaking, Vice Admiral Walter S. Anderson, a former Director of Naval Intelligence, exclaimed "It won the war!" Hyperbole, to be sure, but indicative nevertheless. In fact, a letter of General Marshall, who was certainly in a position to know, tends to support the hyperbole. It was this vital importance of cryptology that was new in the world. No one could have articulated in 1919 the tribute that Representative Clarence B. Hancock offered at the end of 1945 on the floor of the Congress of the United States: "I believe that our cryptographers [cryptanalysts] ... did as much to bring that war to a successful and early conclusion as any other group of men."

For in World War II cryptology became a nation's most important source of secret intelligence.

## 16 Russkaya Kriptologiya

ALTHOUGH SECRET WRITING appears in Russia in the simple letter-substitutions of 12th- and 13th-century manuscripts, akin to those of medieval France and Germany, political cryptography seems to have first come to the country under the Westernizing influence of Peter the Great.

Among the Western innovations that he brought to the new Russia was the exceedingly valuable one of black chambers. Situated, like those of England, France, and Austria, in the post offices, they employed the full battery of expert openers, seal-forgers, translators, and cryptanalysts. At least some of the latter appear to have been German, and their descendants seem to have maintained a monopoly in this field for generations, as in the reign of Peter's daughter, Elizabeth.

Thus the French ambassador, Marquis de la Chetardie, knew well that his dispatches were being opened. But they were enciphered, and, in the manner of diplomats everywhere, he felt safe because he thought that the Russians were too dumb to break his cipher. He may have been right about Russians, but three Germans in the black chamber were making mince pie out of it. He erred in writing home with a deplorable lack of gallantry about the Czarina, remarking that she was "given entirely to her pleasures" and was "so frivolous and so dissipated." The interceptions were seen as a matter of course by Count Aleksey Bestuzhev-Ryumin, grand chancellor of the imperial court. He had been waiting to strike back at Chetardie, who had organized a cabal against him because of his Anglophile tendencies. He showed the solutions to Elizabeth, who, blinded by her own French leanings, refused to believe them until he deciphered them in her presence. The next day, June 17, 1744, as Chetardie entered his residence, he was handed a note ordering him to leave Russia in 24 hours. He protested; a Russian began reading him his dispatches. "That's enough," he said, and started to pack.

*Russkaya Kriptologiya ("Russian Cryptology").

341

At the turn of the century, cryptanalytic information was still informing Russian foreign policy. Foreign Minister Panin wrote on March 26, 1800, from St. Petersburg to his ambassador in Berlin: "We possess the ciphers of the correspondence of the king [of Prussia] with his charge d'affaires here: in case you suspect [Prussian Foreign Minister Count Christian von] Haugwitz of bad faith, it is only necessary to get him to write here on the subject in question under some pretext, and as soon as his or his king's dispatch is deciphered, I will not fail to apprise you of its content."

Twelve years later, Russian cryptanalysis played an obbligato to the grand symphony of the Russian winter in inflicting the first defeat on the hitherto unconquerable Napoleon. That military genius, though not quite the cryptologic moron that it has been the fashion to portray him as being, certainly did not fully appreciate the importance of a tough cryptography. He depended upon a single, easy-to-solve system during most of his campaigns, including the Russian; this was his petit chiffre, a nomenclator of about 200 groups. Even without his generals' predilection for partial encipherments, the Napoleonic cryptograms must have crumpled before the assault of the Russian cryptanalysts. How the solutions helped the Russians is not known, but that they must have been of some assistance is indicated by the fact that the victorious Czar, Alexander I, cited them himself when reminiscing about the war. At a state dinner that he gave in Paris years later for the marshals of France, he mentioned having read secret French dispatches. Marshal Macdonald, who had commanded a corps for Napoleon, recalled that one of the French generals had defected and said, "It is not surprising that Your Majesty was able to decipher them; someone gave you the key." Alexander denied it. "He assumed a serious air," Macdonald related, "placed one hand on his heart and raised the other. 'No,' he replied, 'I give you my word of honor.' " His cryptanalysts would have been proud of so stout a defense of their honor.

During the nineteenth century, cryptanalysts functioned as one of the Czar's chief tools of despotism. Libertarian movements were growing increasingly restive and radical. One way in which the Okhrana, the notorious secret police, kept tabs on underground workers was to have the black

chambers read the letters and telegrams of suspects—as well as most foreign mail and a random selection of the domestic post, too.

The most popular cipher of the Russian underground seems to have derived from the prisons in which so many of its leaders had to serve time. Intercommunication among the inmates was strictly forbidden. But the prisoners, languishing in the tomblike solitude of their gloomy stone casements, with nothing to occupy their minds, had the patience, perseverance, and ingenuity to outwit their jailers. They knocked, using the number of taps to indicate the rows and columns of a simple checkerboard, like the original Polybius square, sometimes 6 X 6 to accommodate the 35 letters of the old Russian alphabet, more often five across and six down, with the alternate letter forms eliminated. In English, the checkerboard would take this form:

abode f g h ij k 1 m n o p q r s t u *v w x y z*

Thus *hello* would become 23 1531 31 34. Prisoners quickly memorized the proper numbers and "talked" at from 10 to 15 words a minute. The system was universal in the penal institutions of Russia, with felons as well as political convicts employing it. ,

One of its advantages was that it afforded communication by a great variety of media—anything that could be dotted, knotted, pierced, flashed, or indicate numerals in any way could be pressed into service. It often concealed a message within an innocuous handwritten letter. The ciphertext numbers were indicated by the number of letters written together; breaks in the count were indicated by minute and almost imperceptible spaces, much as occur naturally in many persons' handwriting. Spaces between Words were bridged by having the last letter of a word ᵉnd in an upstroke if the count was to continue, in a downstroke if the end of the word coincided with the end °f a count. This subtle means, in which the cover-text bears no relation to the underlying message, and so does

not have to strain to make sense, frequently bootlegged secrets in and out of prisons, and undoubtedly past the noses of the black chamber experts, until they finally caught on.

The popular cipher that the checkerboard inspired is named for the Nihilists, the anarchistic opponents of the czarist regime, who may have invented it. The Nihilist cipher converts both the plaintext and a repeating keyword into numerical form via the checkerboard, and then adds them together to produce the ciphertext. If the keyword is ARISE, or 11 42 24 43 15, the plaintext *Bomb Winter Palace* would be enciphered like this:

*literal plain numerical plain key*

*ciphertext*

bombwinterpalace 12 34 32 12 52 24 33 44 15 42 35 11 31 11 13 15
11 42 24 43 15 11 42 24 43 15 11 42 24 43 15 ll

23 76 56 55 67 35 75 68 58 57 46 53 55 54 28 26

Occasional three-digit groups will occur, as 55 -j- 54 = 109. The cipher is a kind of modified numerical Vigenere with additional weaknesses that simplify solution. It would not have baffled an expert very long. Yet this basic system—the adding of a key to a checkerboard substitution, though with important improvements—survived through the years to become the primary form of secret communication for Russian undercover agents.

The Russian plan of campaign against Germany in 1914 called for an invasion of East Prussia by two armies. The 1st Army was to drive straight west into that province and grip the German defenders tightly in battle. The 2nd Army, to the south, was to circle around the Masurian Lakes, come up behind the Germans, block their retreat, and destroy them. This strategy naturally required careful timing and close collaboration between the two forces. Unfortunately, Russian communications were woefully inadequate. The 2nd Army had only 350 miles of wire all told to string during its advance across the plains of Poland; this pitiful supply contrasts sharply with the 2,500 miles of wire later used in a single day by an A.E.F. army on the Western Front. At the same time radios were issued only to the headquarters of both armies and the headquarters of their immediate subordinates—their corps. Division and lower headquarters lacked them. The several corps headquarters therefore used their wire to link up with their

divisions. Since army headquarters had exhausted their meager wire supplies in stringing lines to the rear commands, this left wireless as the only means of communication among the several corps headquarters and between them and their army headquarters—the two highest echelons of field command.

Their messages lay naked to the enemy. The general inefficiency that crippled the Russian mobilization had fouled up distribution of the new military cipher and its keys. Within a single army (the 2nd), for instance, the XIII Corps did not have the key needed to read cryptograms from its immediate neighbor, the VI Corps. The war broke out August 4. Before a fortnight had passed Russian signalmen were no longer even trying to encipher messages, but were passing them over the radio in the clear.

In accordance with the Russian strategy, General Pavel Rennenkampf, commanding the 1st, or northern, Army, began moving into East Prussia on August 17. The German general staff had long foreseen the two-pronged attack—the terrain made it obvious. They had left only one army to defend East Prussia because their strategy called for a quick and decisive victory against France first. This single force was approximately as strong as either Russian army but desperately weaker than both combined, and the general staff had dictated as its strategy to strike with all possible strength at the first Russian force within reach, then to turn and attack the second. East Prussia was the homeland of the Junkers. The Germans preferred not to yield it to the hideous trampling of the Slav.

They gave battle to Rennenkampf at Gumbinnen. Under a hammering Russian artillery barrage, the German troops broke and fled 15 miles to the rear before they could be halted. The frightened German commander prepared to fall back to the Vistula River and abandon East Prussia. He reported his intentions to the German high command, which promptly began looking for a replacement. But his brainy First General Staff Officer, Colonel Max Hoffmann, pointed out that the southern Russian army had already invaded so far that its left wing was actually closer to the Vistula than the German rear and so was in a position to cut off the German retreat. He convinced his chief that he had to strike against this wing to give the German army freedom to maneuver, if only to reach the safety of the

Vistula. The Germans had somewhat mauled the Russian bear before their rout, and Rennenkampf, instead of pursuing to turn victory into triumph, had paused to lick his wounds. Hoffmann was confident that he would rest another day or two. He proposed, and his general agreed, to disengage two German corps from the front against Rennenkampf, switch them southward over the excellent network of German railroads, and fall upon the Russian southern prong with surprise.

The movement was in its early stages when the new German commander, Paul von Hindenburg, and his chief of staff, Erich Ludendorff, who really ran the show, arrived and confirmed it. The difficult entrainment process began. Ludendorff flung out a screen of cavalry along the northern battle line to conceal the withdrawal of his troops and to keep Rennenkampf under observation. The division of forces violated the German strategic doctrine of concentration, and the question arose as to whether all German forces should be thrown into the battle against the southern force, commanded by General Aleksandr Samsonov. To do so would almost ensure victory, but it would also leave the German rear entirely unprotected from an attack by Rennenkampf. While the German staff was discussing the pros and cons of this move on the evening of August 24, a motorcyclist brought in two Russian intercepts. They had been forwarded on the initiative of the head of the radio station at the German fortress at Konigsberg. His operators, who had little traffic of their own to transmit, had begun listening in to the Russian transmissions as a diversion.

Both messages were from the headquarters of Samsonov's XIII Corps, which was communicating with army headquarters by radio because that was the only means the corps had. And both were in the clear because XIII Corps had never received the proper cipher key. They specified exactly where the corps was going, when it expected to be there, and what it would do next. Was it a trick? No, because these details were perfectly consistent with an overall Russian directive that had been found in the wallet of a dead Russian officer the day before. The intercepts did not answer the crucial question of Rennenkampf s intentions. But Ludendorff decided that, with this intelligence, the likelihood of overwhelming victory over Samsonov was worth risking defeat by Rennenkampf. The orders went out

to march the remaining troops facing Rennenkampf across the short inner distance between the two pincers.

The march was getting under way next morning as Ludendorff and Hindenburg appeared at headquarters in Marienburg. But Ludendorff was not entirely free of anxiety about what he had done; second thoughts disturbed him. His thin line of cavalry could have been easily pierced by the Russian 1st Army. "Rennenkampf's formidable host hung like a threatening thundercloud to the northeast," he worried. "He need only have closed with us and we should have been beaten." Their defeat would have meant a tremendous moral blow to the German cause, loss of the country's richest grain and dairy lands, and possibly the fall of the only barrier between the Russian steamroller and Berlin. Should he perhaps have been a little more cautious? While there was yet time, should he leave some troops to block Rennenkampf? Or should he even call off the whole offensive against Samsonov and turn back against Rennenkampf? So much was at stake, and it rested upon little more than his soldier's intuition that Rennenkampf would merely crawl forward as he repaired his supply lines and refitted his troops.

But at headquarters that morning there arrived what at one stroke lifted the burden from the minds of Ludendorff and Hoffmann and permitted them to prepare one of the great military triumphs of the war. It was a Russian intercept. It, too, was in clear, but this one was from Rennenkampf to his IV Corps, and it read, in part:

> The army will continue its attack. On August 25 it will reach the Wiberln-Saalau-Norkitten-Potauren-Nordenburg line; on August 26 the Damerau-Peters-dorf-Wehlau-Allenburg-Gerdauen line.

Their maps told the Germans that Rennenkampf was still moving at his snail's pace. The evidence of hasty German departure that the Russian general had seen as he advanced leisurely upon their evacuated positions had confirmed his erroneous opinion that the Germans were in full retreat after Gumbinnen. He did not want to press them too much for fear of forcing them to the Vistula before Samsonov could crush them. The Germans, however, saw at once that he could not reach any position in time to attack the German rear before the expected destruction of Sam-

sonov *was* complete. Relieved, they concentrated at once on engineering that destruction.

Later that morning, as the German commanders were returning to headquarters from a conference at a corps headquarters, they stopped at a railway station in Montovo for news. A signalman handed Hoffmann still another Russian intercept—also in clear. Samsonov had sent it to the cipherless XIII Corps at 6 a.m. It was a long dispatch, and Hindenburg and Ludendorff had already driven off when Hoffmann got it all. He sped after them in his own car, overtook them, and, as the two automobiles jounced side by side along the rutted Polish road, handed it over. Hindenburg stopped his car, and the officers studied it:

> ... On 25 August the 2nd Army proceeds to the Allenstein-Osterode line; the main strength of the army corps occupies: XIII Corps the Gimmendorf-Kurken line; XV Corps Nadrau-Paulsgut; XXIII Corps Michalken-Gr. Gardienne .... The I Corps to remain in District 5, to protect army's left flank ....

It was, in fact, nothing less than a full roundup of the situation as Samsonov saw it, together with the most detailed and explicit moves to be followed by his army. It gave the Germans a knowledge of enemy intentions unprecedented in the whole of military history. It was like reading the mind of a chess opponent, like playing blind-man's bluff without the blindfold. It was almost impossible to lose.

The Germans formulated their plans to take advantage of the weaknesses of the Russian dispositions. They plotted a double envelopment of Samsonov, and it worked to perfection. General combat opened the next day, the 26th. One of the German corps marching down from Rennen-kampf's front struck hard at Samsonov's right; during the night, that wing was turned. Before dawn on the 27th, a hurricane barrage of artillery demoralized the hungry, tired troops of his left flank, and before noon they had fled the field without a single serious German infantry assault. Soon the realization penetrated to Samsonov that instead of the Russians crushing a retreating German Army, that army had in fact almost enveloped him. His XIII and XV Corps, in the center, fought bravely in the confused, surging struggle, but the frantic orders and cries

for help that their radios squealed in clear were all heard by the Germans who, fully informed, could exploit a gap here, a movement there. Bit by bit the Germans drove in behind the two corps from both sides; soon the Russians found themselves fighting both front and rear. By the 30th, the Germans had encircled the corps with a ring of steel from which only 2,000 Russians escaped. This ended the battle: there were no Russians left to fight. By then Samsonov was dead. He had shot himself in despair as he stumbled through the forest in the night of defeat.

Gradually, it became clear to the Germans that they had won, as Hoffmann wrote, "one of the great victories in history." Almost 100,000 Russians were taken prisoner. An estimated 30,000 were dead or missing. The Russian 2nd Army had ceased to exist. One of the few battles of the entire war that was a decisive victory, Tannenberg—as the Germans named it—demonstrated that the Russian steamroller was not quite the invincible machine that had terrorized central Europe. It catapulted Hindenburg to a popularity that carried him, later in the war, to supreme command, and, in peace, to the presidency of his country. Pro-German groups in Russia began to agitate for a withdrawal from the war. Russian morale sank.

Hoffmann, the architect of the victory, acknowledged its real cause. "We had an ally that I can only talk about after it is all over—we knew all the enemy's plans. The Russians sent out their wireless in clear." The case was clear-cut. Interception of unenciphered communications had awarded the Germans their triumph. Tannenberg, which gave Russia the first push on her long slide into ruin and revolution, was the first battle in the history of the world to be decided by cryptologic failure.

So inexhaustible were the manpower resources of Russia that not even a debacle like Tannenberg could cripple its war effort. "We are happy to make such sacrifices for our allies," replied the Grand Duke Nicholas, commander in chief of the Russian armies, when the French ambassador expressed his condolences. And even though the Germans turned on Rennenkampf and drove him out of East Prussia in the Battle of the Masurian Lakes, two Russian armies pounded the Austro-Hungarian forces back through Lvov with such force that they retreated almost to Krakow. Meanwhile, though stiE plagued with shortages of all kinds,

I

gM|Ui||

including signal equipment, the Russians finally managed to distribute their cipher system to all commands by the middle of September. On the 14th, the Stavka, the Russian high command, prescribed its use for all military orders.

The system was a numerical polyalphabetic which negated most of the advantages of polyalphabeticity by enciphering several letters in succession in a single cipher alphabet. It resembled a feeble cipher used by Cornwallis in the American Revolution and solved with ease by James Lovell. Along the top of its tableau were listed 33 letters of the Russian alphabet; the tableau proper consisted of eight lines of two-digit numbers in mixed order. Each line differed from the others, and they were numbered at the left in mixed order. In enciphering, these cipher alphabets were used in rotation, the one numbered 1 first, the one numbered 2 second, and so on. Each alphabet enciphered several letters at a time. The number of letters to be enciphered in a given alphabet before the next came into play lay at the whim of the encipherer, who informed the decipherer of this number by writing it out five times and then placing this group at the head of the cryptogram. If he wished to change this number during a message, he simply repeated the new encipherment group length five times, inserted it into the body of the cryptogram, and used that length from then on.

Cryptograms in the Russian Army cipher thus consisted of groups of monoalphabetically enciphered letters, with the length of the groups clearly indicated by the unmistakable appearance of, say a 99999 (the maximum length) or a 66666. Aside from being vulnerable to the usual techniques of frequency analysis, the cipher would often mirror the telltale repeated-letter pattern of an underlying plaintext word, such as *attack* or *division,* that had fallen entirely within a single encipherment group and so had been monoalphabetically enciphered. Such a system does not interpose insuperable difficulties to the cryptanalyst, especially when, as with the Russians, it was poorly used, often with intermixture of plaintext. Mixed text was soon prohibited, but by then it was too late.

For the brilliant young Captain Hermann Pokorny, head of the Russian subsection of the Austro-Hungarian Dechif-frierdienst, had cracked the system and reconstructed all its alphabets by September 19. His first important solution, on September 25, disclosed General Novikov's lengthy

report of his reconnaissance of Central Powers troops, with his additional note: "I took the decision of not crossing the Vistula." The message was dated 8:40 a.m.; by 4 p.m. the Austrian liaison officer had brought it to the attention of the German headquarters. Knowledge of Novikov's decision determined the initially successful Austro-German tactics of the battles of the Vistula and San rivers. Other intercepts were valuable in more local situations. A message of Prince Engalitschev, colonel of the 10th Russian Cavalry Division, warned of a strong attack on the fortress of Przemysl; the prepared commander easily warded it off until the Austrian advance forced the Russians to lift the siege in mid-October. During this advance, Pokorny's group solved as many as 30 cryptograms a day.

It was at about that time that the Russians made their first key change. It apparently consisted only of altering the order in which the cipher alphabets were to be used, the alphabets themselves remaining unchanged. Solution of this would have taken Pokorny at most a few minutes. Any difficulty that he might have encountered evaporated when a Russian station repeated in the old key a message already sent in the new.

Meanwhile, the Germans had, more by fortune than by foresight, developed a cryptanalytic service of their own. Ludwig Deubner, a professor of philology at the University of Konigsberg who had enlisted in the Landsturm as an interpreter of Russian and who was stationed at the Konigsberg fortress, began his radio-intelligence work by translating the cleartext intercepts that the fortress radio station picked up. As words in cipher began to appear, he undertook to solve them. Gradually he mastered the Russian system so that he could read messages entirely in cipher. At the end of September, he was called to headquarters and given charge of a group of interpreters who were to learn cryptanalysis. Soon he and Lieutenant Alexander Bauermeister—Hoffmann called them "quite geniuses in deciphering"—were, with their neophyte code-breakers, sending a stream of solutions to Ludendorff each night about 11. The chief of staff waited for them impatiently, barking, "Any radiograms?" at his subordinates. He based his orders for the next day in large measure on the intelligence the intercepts gave. When they were late, he would stalk into the cryptanalytic section to find out what the delay was. And if for a time nothing of im-

portance appeared in the messages, he would growl that the intercept service had not been paying attention.

Such occasions were rare. Direct telegraph connections were soon established between Pokorny's group and Deub-ner's; together they laid open virtually every Russian cryptogram that their posts intercepted. And they were guaranteed a good harvest when the headquarters of a Russian army was given permission to use radio for its front-line activities because its linemen were busy with repair work.

Thus it was that the Central Powers learned from Russian wireless that the Grand Duke Nicholas was forming a huge phalanx of seven armies to rumble into the industrialized heart of Silesia in east-central, Europe. By the end of October, the picture of the composition, disposition, and strength of the Russian forces that Hindenburg and Ludendorff had before them could not have differed much from the official one at Stavka. Only the date of the advance was unknown, but the Germans assumed that it would take a little time before this ponderous Russian steamroller could get up momentum. They determined to seize the initiative and attack first in the hope of throwing a monkey wrench into the steamroller's mechanism.

Ludendorff's plan was characteristically bold. He removed a German army from the defenses blocking the invader and poised it in the north for a plunge downwards into the right side of the Russian wedge. On November 11, the point of this dagger—an army under Mackensen—began to pierce the Russian flank. At 2:10 p.m. the next day, the chief of staff of one of the Russian armies under attack transmitted a long radiogram which the Central Powers intercepted. In addition to mentioning the date of the projected Russian advance, it specified the line of demarcation between his army and a neighbor—always a zone of weakness. This message lay, cryptanalyzed and translated, on the desks of the German headquarters for the Eastern Front at Posen by the next afternoon.

It was immediately forwarded to Mackensen. At 7:30 p.m., with this picture of the Russian dispositions before him, he telephoned his order for the next day to his subordinates. It called for an all-out attack, concentrating on the meeting line of the two armies in the hope of driving them apart and breaking through.

He achieved a massive success. The Russian forces were

split; they pulled back hastily to the south. Mackensen shoved the dagger in up to the hilt. At the same time, Ludendorff pinned the front Russian armies in combat and sent a corps to turn the Russian left flank. He hoped to effect another Tannenberg—a double envelopment. In sharp fighting around Lodz, the German forces drove their enemy back, abetted by a constant stream of cryptanalyzed intelligence. On November 15, for example, the German command learned that four corps were to reinforce Russian troops at the Ner and Bzura rivers and that another corps was to cross to the left bank of the Vistula at Plozk. These details enabled the Germans to maneuver each day as if in a war game.

By now the Russians were changing the key to the order of the cipher alphabets—not the alphabets themselves— each day. The cryptanalysts kept pace. On November 18, it appeared that the Germans had won their victory when the cryptanalysts solved a message ordering a Russian retreat from Lodz. But the rejoicing at headquarters was cut short when the codebreakers read a message from Grand Duke Nicholas countermanding the order and directing his forces to fight on despite their difficult position. The flow of radio intelligence continued unabated, and on the 19th Mackensen even delayed giving an order until intercepted information was received.

The next day a premonitory fear chilled the intercept services when they picked up a message from a liaison officer of the Russian 4th Army to a colleague, warning that the Germans had the Russian cipher key. The Russians had captured a German cipher key, and they apparently assumed that one of theirs had likewise fallen into German hands. A new key was instituted—and this time the entire set of cipher equivalents was changed. A curtain of silence descended upon the Eastern Front.

Feverishly, Deubner and Pokorny, who was assisted by Lieutenant Colonel Heinrich Zemanek and Lieutenant Viktor von Marchesetti, grappled with the new key as the intercept posts sucked in every scrap of Russian wireless. The moment could not have been worse. The battle around Lodz raged at its peak, and just as Ludendorff was about to consummate his envelopment with his inferior forces but his superior intelligence, that intelligence was abruptly blanked out. Deprived of his eyes and ears, he did not know °f the Russian reinforcements that began to cut off the

deeply sunk point of Mackensen's dagger. By the 21st, the point had been isolated, and the envelopers were themselves enveloped. A guards division and two cavalry corps were encircled by Russian forces with no apparent hope of escaping. The Russians exultantly ordered up trains to carry off the prisoners.

But the next day, Pokorny's group finally subdued the new Russian alphabets, and the intelligence once again began streaming into German headquarters. Intercepts soon revealed a weak spot at Brzeziny in the ring of Russians. Ludendorff's headquarters radioed this information to the trapped commanders, who, grouping their forces densely and fighting hard, broke out on the 25th and reached safety, bringing with them 10,000 prisoners. General Lietz-mann, commander of the guards division, won the title "Lion of Brzeziny" for the brilliant escape; the crypt-analysts who had showed him how best to use his fangs and claws purred with amusement in their secret lairs.

This harrowing episode, resulting from a fortuitous change of key, balked the Germans of a decisive victory, but they had succeeded in throwing the vaunted Russian steamroller out of gear. Never again did it threaten German soil. The Central Powers pressed forward, still reading Russian cryptograms, and on December 6 the soldiers of the Czar evacuated Lodz, the second city and the industrial capital of Poland. Eight days later they again made a wholesale change of alphabets in their digit cipher. Solution again required several days, and when it was completed the Austro-German command learned that the Russians planned to dig in for the winter along the Nida River. Soon thereafter they gave up the old cipher altogether.

When activity quickened in the spring of 1915, the Russians were using a simple Caesar cipher.* The multiplicity of tables used by different armies in the old cipher, the daily shift of keys, had evidently proved too difficult to handle for the half-illiterate muzhiks. The Austrian and German cryptanalytic organizations saw right through this transparent new cipher and read the indications of a projected Russian invasion of East and West Prussia. Then began what Colonel Max Ronge, head of Austro-Hungarian

*During the Second Battle of the Masurian Lakes in February, in which the Russians were defeated, they used a service code called the RSK, which the Germans solved. Its nature is unknown.

intelligence, called "the most brilliant period of our interception services." Enormous quantities of intelligence were sluiced from the Pokorny and Deubner groups into the offices of the operations staffs of the German and Austro-Hungarian commands. Helped by this, they parried the first tentative Russian advances, and then themselves swept through the whole enemy line in a rapid onslaught that penetrated 80 miles in two weeks.

Time after time, their solutions enabled the Central Powers to take steps which were so perfectly the right thing to do in each tactical situation that the Russian general staff was mystified by its opponents' apparent clairvoyance. Once the Germans fell back just two days before an overwhelming assault was to be launched; had they remained in place, their position would quickly have become critical. After the Germans captured Lodz, the Russians pondered the precision of the enemy moves and decided that the Germans must have obtained intelligence from air reconnaissance.

Eventually, however, the conviction grew that the foe must be reading their ciphers. They did not suspect crypt-analysis. Spies, they thought, must have sold them to the Austrians, and in a wave of spy-mania they persecuted officers with German names—none of whom, Ronge said, had ever given anything to him. The Russians changed their cipher at the height of the enemy's spring offensive, but this caused the cipher clerks more trouble than it did the cryptanalysts, for almost all messages of May 15 were unintelligible to their recipients and most of those of the 16th as well.

The summer-long Russian retreat finally came to a halt at the end of September on a defensible position deep within their own territory. By then Russia had lost 750,000 men as prisoners and untold hundreds of thousands more as casualties. She simply threw more men into the war. She seemed to adhere to the same policy in cryptography— and with the same lack of success. On December 20, 1915, she put her 13th cipher into operation. The Austrian and German cryptanalysts recognized it at once as having been used elsewhere on the front, and during the inconclusive battles before and after New Year's Day kept up with the enemy situation hour by hour. On June 16, 1916, the Russians began using their first code, a small one of about 300 groups. This development may have been influenced

by the French, who had learned about the German solution of Russian messages from their own cryptanalyses and had passed the news to their allies. Or it may have resulted from Russia's own intercept service; just how well Russia did in military cryptanalysis is not known, but she did set up direction-finding stations in mid-1916 and started an intercept school at Nicolaieff.

The travail of the Central Powers cryptanalysts, who were unused to code, was simplified when some Russian commands, who were equally unfamiliar with it, continued using the old system. And their work was made almost mechanical when the headquarters of a Russian guard detachment that was being joined to the 8th Army compromised the new system by a message in clear. A great hubbub arose in the 8th Army; a new code was instituted; this one cryptanalysts solved without much trouble. By then they were reading up to 70 Russian dispatches a day. The German solutions seem to have been made in the radio stations of the various fortresses, to which Deubner communicated the keys as he solved them. Some of the Austrian cryptanalysis was done at Ronge's Austro-Nord Penkala under the command of Captain Karl Boldeskul. Later in the war, when Pokorny was promoted to head of the whole Kriegschiffregruppe, the Russian subsection of the Dechiffrierdietist at headquarters was taken over by von Marchesetti; in 1918 Rudolf Lippmann succeeded him.

On November 6, 1916, the Russian Army of the Danube suppressed the radio use of cipher No. 14 as known to the enemy, and on December 17 another cipher was called out of service because the radio station of the 1st Cossack Division had been captured. Four days later they returned to the air with a code that proved to be merely a slightly shifted version of one that had been instituted a week earlier. All these changes the cryptanalysts followed with contemptuous ease. The increasing disorganization of the Russian armies contaminated the radio services, and as discipline relaxed, garrulity increased. One day early in 1917, the Dechiffrierdienst solved 333 radiograms, from which it inferred that the Russian secret communications were rapidly disintegrating. In March the Czar-was overthrown, in July an all-out offensive by the Russian armies collapsed, and in October the Bolsheviks, using the people's overwhelming desire for peace, seized power and took Russia out of the war.

The way to this situation was opened primarily by Russia's military failure. While this resulted largely from the lack of munitions, food, and supplies that the underin-dustrialized country could not supply, the tactical defeats inflicted by the Central Powers obviously played a conclusive role. And these victories of a David over a Goliath, though aided by superior German equipment, discipline, and logistics, were mainly engendered by cryptanalysis.

"We were always warned by the wireless messages of the Russian staff of the positions where troops were being concentrated for any new undertaking," wrote Hoffmann. So complete was the intelligence that he could say: "Only once during the whole war were we taken by surprise on the Eastern Front by a Russian attack—it was on the Aa in the winter of 1916—17." This dramatically underlines the importance of cryptanalysis in the outcome of the war in the East and in all that that entailed. Indeed, it may not be too much to claim that the establishment of Communist power, perhaps the supreme fact of contemporary history, was made possible to a significant degree by the cryptanalysis of czarist secret communications.

The consolidation of the Soviet regime permitted Lenin and his colleagues to turn not only to the difficult problems of running the world's first socialist state but also to the traditional Communist activity of fomenting class struggle and the revolution of the proletariat. They felt justified in using subversion as well as the more orthodox methods of propaganda and political agitation in advancing Marxism in countries that had not yet reached Russia's stage of historical development.

It was during the Spanish Civil War, in which Russia actively aided the Loyalists, that a cryptographic element that had served the revolutionary predecessors of Lenin & Co. reappeared in a form both streamlined and more secure. This was the straddling checkerboard. Its straddling feature makes use of cipher equivalents of two different lengths—lengths usually of one digit and two digits; the two sets of equivalents are so constructed that the cryptographer can unambiguously separate them when they are run together. The cryptanalyst, however, not knowing which digits are singletons and which form,pairs, may divide the ciphertext incorrectly, thereby "straddling" many of the true pairs and combining two singletons into a false

pair. The device also reduces the length of the numerical text as compared with checkerboards in which all letters are replaced by numerical pairs. Straddling was first employed by the Argentis in some of their 16th-century papal ciphers (one wonders whether the atheistic Communists knew!).

The straddling checkerboard produces single-digit equivalents by leaving the side coordinate off one of the rows of the checkerboard. A letter in this row is enciphered by just the single coordinate above it. If ambiguity is to be avoided, none of these singletons can start a two-digit group. Hence none caa be used as a side coordinate (which is read first). Using eight digits of the ten as singletons leaves two digits as side coordinates;, each of these two side coordinates can then pair with the ten top coordinates (the singletons may serve in second position) to produce 20 two-digit groups. This configuration makes 28 ciphertext equivalents available for plaintext elements.

It was used in 1937 with keyword M DEL VAYO, the M the initial of the agent, the DEL VAYO the name of a Spanish Communist. The two extra spaces were used for a period and a letter-number shift sign:

0987654321

mdel v a y 6 bcf ghuj knp qrstuwxz. /

With this, *e* = *8*, *a* = *5*, *b* = 10, *t* = 27, and so on. There will be no single 2 or 1. The decipherer takes all 1's and 2's as the first digits of a two-digit group, and joins to it whatever digit follows. He takes any digits from 3 to 0 as individuals if they are not already part of a pair. Thus the ciphertext 828115125 can be unambiguously divided as828115125 and deciphered to *Espana.*

Other configurations are possible. Seven single digits will permit three side coordinates, for a total of 37 cells in the checkerboard. Six singletons will produce 46 cells; five, 55, and so on down to one singleton, 91 cells. The arrangement with 28 equivalents has been widely used for Latin-alphabet texts, that with 37 for Cyrillic texts.

Although the M DEL VAYO checkboard was used by the Swedish fellow traveler Dr. Per Meurling only to teach his fiancee secret writing, his knowledge of it testifies to

its use at that time by the Communists. He subjected the numerical text resulting from the checkerboard to a multiplication, and then reconverted the product to letters in another checkerboard. The system resembled but was much weaker than Pliny Earle Chase's of 1859, and it is unlikely that the Russians would have used it in that form.

The Spanish Civil War, a prelude to World War II, furnished the Fascist-Nazi and the Communist dictatorships with a testing ground for the weapons they would use in the later conflict. Perhaps this extended—for the Communists,, at least—to the cryptologic arena as well. Red ciphers of World War II had purged themselves of whatever weaknesses were discovered in Spain and had erected upon their strengths an impregnable structure.

Any suspicious letters were turned over to the chief cryptologic agency of the Soviet Union, the quasi-independent Spets-Otdel ("Special Department"), whose primary task was reading the coded messages of other nations. Though attached to the foreign directorate of the secret police, it was actually responsible to the Central Committee of the Russian Communist party, the Soviet

.. Union's real ruling body, whose chairman was first Lenin and then Stalin. In 1938, it appears to have been renamed and reorganized into the 5th Directorate of what was then the N.K.V.D.

Up until that time, and beginning, apparently, around 1927, its chief was Gleb I. Boki, an old Bolshevik and friend of Lenin, who, at the same time, sat on the Supreme Court of the Soviet Union! Born in 1879, he had taken part in prerevolutionary activities and had gained the Communist badge of honor by being arrested many times and winning a three-year sentence in Siberia. At the time of the Revolution, he was secretary of the Bolshevik cell in the capital, St. Petersburg. In the early 1920's, he headed the Cheka in Turkestan, where he so terrorized the country that legends about him remained alive long after he had gone: that he ate dog meat (especially execrable to the Moslem population), even that he drank human

, blood. It seems true, however, that as head of the Spets-Otdel Boki held wild parties, if not actual orgies, with a group of carefully selected guests at his rented dacha near Batumi during his vacations. He kept his office door always

i closed and used a peephole with one-way glass to examine

visitors. Tall and stooped, with a sinister expression and cold blue eyes that gave one the impression that he hated the very sight of you, he gave at least one girl worker the shivers whenever he emerged from his sanctum and spoke to her when she was alone in the office on night duty. Never with a hat and always with his raincoat, which he wore in all seasons, Boki seems to have been an administrator rather than a cryptologist. He was executed in 1938 in the great Stalinist purges. Afterwards, it was discovered that he had, most unsocialistically, hoarded gold and silver coins.

The Spets-Otdel handled both cryptography and crypt-analysis. In 1933, the cryptographers worked in a big room on the fourth floor of a former insurance building that the O.G.P.U. occupied at 6 Lubyanka Street. The cryptanalysts were then on the top floor of a former Ministry of Foreign Affairs building at the corner of Lubyanka Street and Kuznetsky Bridge Street. The comings and goings of ordinary tenants on the lower floors and of the members of a diplomats' club disguised the presence of the office. In 1935, both cryptographers and cryptanalysts moved into the new building of what was now the N.K.V.D. at 2 Dzerzhinsky Street (named for the first head of the secret police, Felix Dzerzhinsky).

The cryptographic division was subdivided into several sections. There were separate sections, for example, for the N.K.V.D. network inside Russia, for the border patrols (under N.K.V.D. jurisdiction) and uniformed N.K.V.D. troops, for Gulag, the prison administration, for clandestine agents abroad, and for the "legal" N.K.V.D. residents abroad. This last section was No. 6. Its chief, Koslov, was dismissed during the purges, and after his successor was sent to the United States as a cipher clerk, the section was headed by a man not unknown to later fame—Vladimir M. Petrov, who defected in 1954 and was granted asylum in Australia,*

*Petrov named three men who were his bosses at different times while he was section chief—Ilyin, Degtjarov, and Shevelev. Whether these were the heads of the entire, then newly formed N.K.V.D. 5th Directorate, or whether they were department heads (a possible administrative level between the section chiefs and the directorate's chief), is not known. The former may be more likely in view of the fact that Boki's successor, Shapiro, lasted only a month or two before he was arrested, and three or four of Shapiro's successors were also arrested.

The growth of Section 6 may measure that of Soviet espionage. When Petrov joined in 1933, there were only 12 workers; in 1951, there were 45 or 50. As cipher clerks in the N.K.V.D., entrusted with the deepest secrets of the most secret agency in Russia, these people were among the elite of the Soviet Union, yet their jobs in this workers' paradise were anything but heavenly. Ciphering was done by hand, and early in his career Petrov often worked until midnight to clear up the day's backlog of telegrams. Later, as deputy section chief, Petrov did no actual enciphering or deciphering, but read the telegrams, corrected them, and signed them.

The cryptanalysts were divided into geographical and linguistic subsections—Chinese, Anglo-American, and so on.* The future Mrs. Ekdovia Petrov, who had studied Japanese for two years at a language school in Moscow, was assigned to the Japanese section. Among her co-workers were Vera Plotnikova, daughter of a professor of Japanese and a long-time resident of Japan; Galina Pod-palova, who liked things Japanese so much that she wore kimonos at home; Ivan Kalinin, who came in occasionally as a consultant; and Professor Shungsky, old, distinguished, vigorous, the section's supreme authority on Japanese. He gave Doosia (the future Mrs. Petrov's nickname) an affectionate kiss on the cheek when, after four years of his tutoring, she translated a difficult sentence to his liking at her final examination.

Shungsky had served in the czarist Army, and many others in the cryptanalytic section were elderly former Russian aristocrats, including counts and barons. This shocking breach of Bolshevik polity resulted from a serious shortage of linguists, who were needed in codebreaking. Cryptanalysts themselves were so excessively scarce that even when they were jailed they continued to work. Vladimir Krivosh, the father of Doosia's first love and de facto

*In 1933, it also had a military intelligence group, headed by a Colonel Kharkevich, a solid, impressive man who reported to both Boki and the general staff. This group appears to have later been abolished or transferred to the Army; Kharkevich himself was Purged in 1938. The head—under Boki—of the O.G.P.U. group of wyptanalysts was one Gusev, possibly Sergei I. Gusev, an old revolutionary, active in secret printing, a member of the Central Committee of the Russian Communist party since 1922, and on the Praesidium of the Comintern from 1930. He too was purged in 1938.

husband, Roman Krivosh, had held a high post in the Okhrana; he was alternately arrested and released, but worked for the Spets-Otdel even while he was in the Butirskaya Prison in Moscow. Eventually the police took Roman away to the same prison, but the head of his section in what was then the 5th Directorate brought him his work.

There was, of course, no security problem with inmate-cryptanalysts. But security was impressed on the others. They were not allowed to tell anyone the department in which they worked nor even where the office was. Doosia never even told her parents. They also had to keep out of restaurants, presumably because their conversations might be overheard.

Did their work prosper? It did, and very well indeed. In 1929 or 1930, the Spets-Otdel compiled a weekly precis of foreign telegrams that it had solved and sent it to O.G.P.U. department heads and to the Central Committee. By 1938, the pace seems to have accelerated, for by then Doosia had the job with a Madame Moritz of checking the typed fair copies that represented each day's output against their handwritten originals. One former O.G.P.U. official stated that the Spets-Otdel "carries on the work of reading codes splendidly" and praised Boki's staffers as "a first-class lot, often cited for emulation."

The strides that the Russian Army had made in cryptography after the traumatic experiences of World War I were dramatized by an interchange of messages between incredulous Russian units at the very start of the Russo-German War. Moments after the Nazis launched their sneak attack at 3:30 a.m. June 22, 1941, a Red outpost wirelessed frantically, "We are being fired on. What shall we do?" Back came the stern reply, "You must be insane. And why is your signal not in code?"

Red Army cryptography rested in World War II upon the enciphered code. The system appeared in four series: 5-digit codes for strategic messages, 4-digit for high-level tactical communications, perhaps of the rank of army headquarters, 3-digit for medium-level tactical, as of brigade rank, and 2-digit for the front. The Soviets replaced their tactical codes frequently, although sometimes a code that had been used in one sector of their thousand-mile front reappeared later in another. The 4-digit codes were en-

ciphered by 10 X 10 tables, one table for the first 2 digits and another for the second pair. The 5-digit codes were enciphered by additive tables of 300 groups changed daily. The Army and Navy shared the 5-digit strategic system; border patrol and N.K.V.D. units had their own systems, usually 4-digit. In addition, the Soviets got some Hagelin M-209s in Lend Lease, which they apparently used as models for their own constructions, though it is not known where these were used.

With enough traffic, enciphered code can of course be read. One of the first to do so in the case of the Russian military was the Swedish expert Arne Beurling. During the bitter struggle of Finland against Russian aggressors in the Winter War of 1939-1940, Sweden fed intelligence based on cryptanalysis to her neighbor. Beurling attacked the top system, the 5-digit strategic, which was actually a 4-digit code with an extra digit added as some form of check. In several of the codes, the page digit—the second— was repeated, so that the groups would look like 52217, 88824, and so on. In others, the fifth digit gave the unit total of the preceding four digits, so that 6432 would have a check digit of 5, making the codegroup 64325. Beurling wrote the cryptograms on a sheet of graph paper with five-millimeter squares that was so large—about 3X4 feet —that he had to order it specially. He sought to strip the superencipherment and, with luck, sometimes succeeded.

Soviet strategy against Finland called for a five-pronged invasion along their north-south border. The middle force drove for the tiny village of Suomussalmi to cut Finland at her waist; the force just north of that one rolled on another little village, Salla, in a secondary cut-off. But intelligence developed in the Swedish cryptanalytic office helped the Finns to repulse both Russian attacks.

Crucial to Marshal Mannerheim's victory at Suomussalmi was the information that the Russian 44th Division, a crack motorized outfit from Moscow, was advancing from Raate. He immediately sent reinforcements to Suomussalmi. Two days after his five battalions reached there, the Finns, dressed in white and moving like the ghosts of the north, attacked the Russian forces in the village, broke their resistance, and forced them to flee across frozen Lake Kiantajarvi. The skiing wraiths then cut off the retreat of the 44th Division, severed its column and destroyed it section by section in fighting that continued into the

first week of 1940. Large quantities of stores were captured, but, Mannerheim wrote, "The enemy's casualties could not be estimated, as great snowdrifts over a large area covered the fallen as well as the wounded who were frozen to death."

Temperatures during the battle dropped to 56 degrees below zero, and it was under such conditions that the Swedes solved some pitiful messages from isolated Russian units. One encircled group radioed that they were burning their papers and were going to shoot their last horse for food, and that this was their final message. Silence followed, and soon thereafter the Swedish cryptanalysts learned that the Finns had crushed them. Another Russian battalion sent a coded message that they were desperately short of supplies and would build three fires in a triangle to show the Red Air Force where to parachute desperately needed food and ammunition. The Swedes solved it and gave it to the Finns, who built a triangle of fires and watched with bitter satisfaction as the packages floated down into it.

Swarms of Russian Air Force cryptograms were downed by the Swedish codebreakers. Many were orders to bomb Helsinki, and often these were solved before the bombers took off from airfields in Latvia and Estonia for the 20-minute flight to their target. Finnish authorities thus had ample time to sound air-raid alerts; as a result the capital suffered exceptionally light civilian casualties considering the number of bombs dropped.

But little Finland was no match for the colossal U.S.S.R. despite her cryptologic advantages, and in March she signed a peace treaty. When the Germans invaded Russia a year later, Finland declared war against her harasser and later exchanged cryptographic intercepts with her new ally.

German radio intelligence against the Soviet Union appears to have been characterized by a severe split. Strategically it enjoyed no success at all. The Germans did not solve the cryptosystems of the top Soviet military commands—primarily the 5-digit codes. Perhaps by 1941 the Russians had corrected their cryptographic, technique enough to keep the Germans from repeating the 1939 Swedish successes. Whatever the reason, cryptanalysis contributed little to O.K.W.'s overall picture of Russian strategy.

Tactically, however, the Germans reaped rich harvests of intelligence. In mid-1940, when Hitler first decided to attack the Soviet Union, Germany had no radio-intelligence service of any kind in the East; a year later, when Hitler struck, the new intercept service had already provided him with good information on Russian order of battle. In July, a captured Russian Air Force captain betrayed one of the Air Force systems. This intelligence windfall helped the Luftwaffe destroy hundreds of Soviet airplanes on the ground and another hundred in a great air battle over Minsk.

The resultant air superiority, plus surprise, momentum, armor, and speed, carried the Wehrmacht forward in a surge of victories. In 1941 and again in 1942 Germany mounted massive offensives and overran vast areas of Russia. But in the winter of 1942-43, Stalingrad held and the German 6th Army capitulated; at the same time, Germany lifted the two-year siege of Leningrad. By next summer, it had become evident that Nazidom could not win its great victory over Bolshevism, but the troops hoped at least for a stalemate that would stabilize their conquests. The high command decided on some limited attacks to cripple Soviet offensive power. With the waning of Luftwaffe air mastery, Nazi intelligence had to depend less upon aerial reconnaissance and more upon wireless surveillance. In tactical operations during the Battle of the Dnieper in October, 1943, the chief of staff of the 48th Panzer Corps declared, "The best and most reliable source of intelligence was our Wireless Intercept Service."

A few months later, that corps participated in one of the attacks that Army Group South, one of the three major German groupings on the Eastern Front, mounted to flatten the Kiev salient and further forestall Soviet offensive propensities. The 48th Panzer Corps had as its objective the disruption of the Russian 60th Army. Air reconnaissance produced no information, and the corps decided not to send out ground scouts for fear of alerting the Russians. The attack at 6 a.m. December 6 completely surprised the Russians, who recoiled in confusion.

> In those days [wrote the corps' chief of staff, Colonel F. W. von Mellenthin] we were really good at intercepting Russian wireless traffic; enemy messages were promptly deciphered and passed to Corps in time

> to act on them. We were kept well informed of Russian reactions to our movements, and the measures they proposed to take, and we modified our own plans accordingly. At first the Russians underestimated the importance of the German thrust. Later a few antitank guns were thrown into the fray. Then slowly the Russian Command got worried. Wireless calls became frantic. "Report at once where the enemy comes from. Your message is unbelievable." Reply: "Ask the Devil's grandmother; how should I know where the enemy comes from?" (Whenever the Devil and his near relations are mentioned in Russian signals one can assume that a crack-up is at hand.) Towards noon the Russian 60th Army went off the air, and soon afterwards our tanks overran the army headquarters.

By that evening the Germans had rolled up the Russian front for 20 miles, and by the night of December 9 the Soviets' projected offensive was jolted thoroughly off balance. In the next few days additional blows punished them further. "The Russians were certainly flabbergasted by these ghost-like thrusts, which seemed to come from nowhere, and their wireless traffic provided abundant evidence of their bewilderment and anxiety," Mellenthin wrote.

This German victory at the Battle of Radomyshl delayed but did not prevent the Russian offense. At Christmas, Army Group South began its retreat from the Ukraine. Several months later the Russians had driven the Germans back 650 miles from their farthest penetration.

Mellenthin has remarked that "The Red Army of World War II was vastly different from the Imperial Russian Army of 1914-17, but in two important respects the Russians have not changed. They are still addicted to mass attacks, and they still show an extraordinary indifference to wireless security." This comment seems to hold true only in a tactical sense, and the adjective "extraordinary" is probably justified only under conditions of retreat and its accompanying confusion.

Army Group North, for example, read 5-digit code messages very rarely. Of the intercepts in 2-, 3-, and 4-digit codes, it read 28.7 per cent—13,312 messages out of 46,342 from the beginning of May, 1943, to the end of May, 1944, a year in which the Russians pushed back the northern sector of the front slightly, though not nearly as

much as the southern. A month-by-month and system-by-system breakdown of the cryptanalytic success of Army Group North (excluding 5-digit codes) shows a decline as the Russians improved their cryptographic discipline.

As might be expected, the 2-digit systems, being the simplest, succumbed the oftenest. However, fewer 3-digit than the presumably more difficult 4-digit enciphered codes were solved, even though more 3-digit messages were picked up. The reasons for this seem to lie partly in the probable concentration on the information-rich 4-digit messages, partly in the many more 3-digit systems in use and the consequent difficulty of finding overlaps to strip off the additive and of getting sufficient text for solutions. This multiplicity of 3-digit systems can be seen in the number of new 3-digit systems reported solved each month by the cryptanalysts, which is invariably greater than the number of new 4-digit systems. In November, 1943, for example, Army Group North solved 15 new 3-digit systems as compared to one 4-digit; in December, the figures were 8 and 4, in January, 1944, 15 and 8. The cryptanalysts do not give the number of new systems introduced by the Soviets that the Germans did not solve.

Solved messages, said the cryptanalysts' report for February, 1944, "contain operational combat reports, statements about assembly areas, command posts, loss and replacement reports, reports about chain of command and positions prepared for the attack (e.g., messages of the 122nd Armored Brigade on February 14 and 17). Besides these reports, the plaintexts of the messages made possible the identification of seven armored units, including their numerical designations, as well as confirmation of twelve armored units. With few exceptions the material could be worked up in good time and put to use."

These tactical solutions could, at best, produce local successes. The apparent failure of German cryptanalysts to solve Russia's strategic cryptosystems, with the valuable information that they concealed, led one German crypt-analyst to adjudge that Russia lost World War I in the ether and won World War II there.

A truth he never suspected may lurk in his apothegm. For the Russians may have done as well in solving German cryptograms as in protecting their own. By 1942 they had cracked messages in the Enigma, a rotor machine. And the Germans themselves paid a left-handed tribute to

Soviet cryptanalytic perspicacity when a 1943 conference of signal officers ruefully ordered: "It is forbidden to mark the Fiihrer's radio messages in any special way."

At the same time, the Soviet Union guarded her diplomatic flanks by the one-time pad, a practice she had begun in 1930. Consequently her crucial Foreign Office messages were read by neither foes, nor neutrals, nor allies. Any schemes that she may have instigated against those who, at the end of the war, were to become either her puppets or her adversaries remained among the most inviolate of her secrets.

During World War II, the secret prospectors of the G.R.U. and the N.K.V.D. drilled for information in scores of places all over the world. Three of the spy crews struck gushers of it. The fabulous "Lucy" network in Switzerland, the Rote Kapelle in Germany, and the Sorge ring in Japan pumped a continuous stream of the most detailed and precise intelligence into the Kremlin. And this they did through a pipeline that, despite the most strenuous bang-ings and poundings of counterintelligence, remained hermetically sealed against cryptanalysis. All three rings employed the then-standard Soviet espionage cipher. It achieved a triumph of encipherment, for it is a system that the spymasters of the Soviet Union rightly regarded as unbreakable.

It brought the old Nihilist substitution to a peak of perfection. It merged the straddling checkerboard with the one-time key.

It increased the efficiency of the checkerboard by specifically giving the high-frequency letters the single digits. This cut down the length of the cryptograms and hence time on the air. Both Max Clausen, radio operator for the Sorge net, and Alexander Foote of the Swiss ring, enciphered in English, and consequently they used the eight most common letters of that language. They memorized them by the rather ominous phrase "a sin to er(r)." However, the sequence of those letters played no part in the construction of the key alphabet.

For that construction, a keyword was selected. Clausen used SUBWAY. The encipherer wrote this out, followed by the rest of the alphabet in rows beneath it, with a full stop and a letter-number switch sign at the end. Then the digits 0 to 7 were assigned to ASINTOER as they oc-

curred vertically in columns from left to right. Finally the two-digit groups from 80 to 99 were assigned to the remaining letters and symbols, also vertically:

| | | | |
|---|---|---|---|
| | | | |
| 2 | 7 | 1 | 7 |
| | | | |
| 0 | 3 | 2 | 5 8 |
| | | | |
| 4 | 8 | 3 | 6 |
| | | | |
| 5 | 9 | | 9 |
| | | | |
| 1 | 6 | 0 | 4 |

These equivalents can be placed into the more compact checkerboard:

| 0 | |
|---|---|
| | q |
| | V |

The encipherer next replaced his plaintext with his checkerboard equivalents. For numbers, he enciphered the switch sign, then repeated the digits twice, then enciphered the switch sign again to indicate a return to letters:

whereis/ 1 0 6 / d i vision 91 98 3 4 3 1 0 94 11 00 66 94 83 1 99 1 0 1 2 7

The next step enshrouded this simple text by adding a numerical key—an operation called "closing." Clausen and Foote took their keynumbers directly from a common reference book with many tables, like the *World Almanac,* possession of which would not necessarily be suspicious. Poote used a book of Swiss trade statistics, Clausen the 1935 edition of the *Statistisches Jahrbuch fur das Deutches Reich*—the main section, on white pages, for enciphering, the international survey section, on separately numbered green-tinted pages in the rear, for deciphering.

The message requesting information about the 106th Division resembles one actually sent to the Sorge ring on March 3, 1940. Since Clausen would be deciphering it, it Was enciphered in Moscow with an additive from the green

pages of the *Statistisches Jahrbuch.* The encipherer picked at random the group at the llth row in the 3rd column of page 171. That group happens to give the thousands of metric tons of foundry products fabricated for railroad construction in Luxembourg in 1931, which was 113. The encipherer began, as an enciphering rule required, with the third digit, 3, and then ran along that line in the table, taking his other keydigits from the production figures for Belgium, France, Great Britain, and so on for 1931 and succeeding years: 134, 534, 517, and so on. These digits he wrote beneath the checkerboard encipherment and added them with noncarrying addition to produce the cipher:

*checkerboard* 91983431094110066948319910127 *"plain" key*
31345345171831281196110418847

*cipher* 22228776165941247033429328964

The encipherer divided this into groups of five, 22228 77616 59412 47033 42932 8964, with perhaps a 0 at the end to fill out the group. He then composed an indicator group to tell the decipherer where to find the key: 11 for the row, 3 for the column, 71 for the page (hundreds figures were omitted; presumably the decipherer would have to try page 71 or 271 if page 171's key did not make sense). To conceal this indicator group, 11371, the encipherer added to it, by noncarrying addition, the fourth group from the beginning of the message, 47033, and the fourth group from the end, 59412, to give 07716. He placed this group at the head of the message and gave it to the radioman to send.

This was the standard Soviet spy cipher of World War II. Later in the war, when Foote was enciphering, a few minor improvements had been made to improve reliability and security. Numbers were repeated three times instead of twice. Instead of just one enciphered indicator group, two were used. Foote composed them by adding the plain page-column-line indicator to a fixed group (his was 69696) and then, for the first enciphered indicator, he added this sum to the fifth ciphertext group, from the beginning, and, for the second, to the fifth ciphertext group from the end. He then inserted these enciphered indicator groups as the third group and the third from last group of the final cryptogram.

Russia's wartime allies had never ceased to be her espionage targets, and peace enabled her to concentrate on them again. Soviet espionage scored most spectacularly with the atomic spies Klaus Fuchs and Allan Nunn May, but it did not neglect lesser fry. As the Iron Curtain clanged down and the Cold War grew gelid, secret agents were planted here and there throughout the free and uncommitted worlds. The Soviet spy net covered the globe. To direct it, to protect it, and to harvest its catch, an elaborate system of secret communications was required.

For its secret agents in the field, the Soviet Union uses the best; It takes no chances, cryptologically speaking, with them or their networks. It gives its agents the confidence that they need fear nothing from cryptanalysis. It will not jeopardize their radio links with Moscow by trusting to anything less than the one perfectly secure system of encipherment. The main Soviet spy cipher today employs the one-time pad.

Its form varies. It has been found as a thick, squarish booklet the size of a postage stamp and as a scroll about the size of a cigarette butt. It seems to be growing smaller. A pad captured in 1954 had 40 rows of eight five-digit groups. One captured in 1958 had 30 rows of ten. Pads captured in 1957 and 1961 had 20 rows of four and five groups, respectively. Columns, rows, and pages are numbered. One booklet had 250 pages of a material like very thin gold and silver foil (several scrolls are needed to provide an equivalent supply of key digits). Usually, one part of the pad is printed in red and the other in black, presumably to distinguish the enciphering keys from the deciphering. The "printing" seems to be simple photography —probably the best way to make the one accurate copy of the original key that the agent will need; extra evidence for this is that the Russian word *gamma* ("scale"), which appears to be the Soviet term for one-time pad, is used in photography. Furthermore, the "paper" of the pad is cellulose nitrate, which was used for film in the early days of the motion-picture industry. It is highly inflammable, and spies seem to have kept potassium permanganate at hand to turn an ordinary combustion into an almost explosive reaction to destroy the pads rapidly and completely. No latent image would remain.

One-time pads have turned up with a number of top Soviet spies. Rudolf Abel, the highest-ranking Russian

agent ever captured in the United States, had the one in the form of a booklet and the size of a postage stamp— 1% X % X % inches. F.B.I, agents found it when they arrested him in his room in New York's Hotel Latham on June 21, 1957. Abel had wrapped it in paper and concealed it inside a hollowed-out block of wood covered with sandpaper like a sanding block (Abel posed as an artist) that he had tossed casually into the wastebasket. A Greek Communist, Gregory Liolios, had a one-time pad when he was arrested in 1954, as did another, Eleftherious Voutsas, picked up in 1958. In suburban London, early in 1961, half a dozen one-time pads in the scroll form were found hidden in the base of a Ronson cigarette lighter in the cottage of Helen and Peter Kroger, two Soviet spies who were actually two Americans named Lona and Morris Cohen. More pads were found in another lighter in the London flat of their chief, the Soviet Resident (agent in charge) for England, known only by his alias, Gordon Arnold Lonsdale. Later that year, Japanese police rounded up members of a North Korean Communist spy ring, and found among their effects some one-time pads. Atomic scientist Giuseppe Martelli, accused of espionage against Britain for the Soviet Union, was carrying two tiny packs of pads in a pack of cigarettes when he was apprehended at Southend Airport in 1963. Seven cigarettes were intact, but six others were glued together and partly cut away to form a recess for the pads. And a former spy for East Germany, who received his messages in an open broadcast of numerical codegroups and sent them by leaving them in a tin box hidden under a tree root, also enciphered with the one-time pad.

Though the one-time pad is the standard method for radio communication between top agents and Moscow, other systems serve the internal needs of secret communications within Communist spy rings. The rule here seems to be that where Russians have devised the systems, they are top-notch, and where local Communists who are natives of a country have done so, they can be solved—often with disastrous effect. In 1955, for example, Swedish counterespionage police noticed that a chauffeur at the Czech legation went to the Stockholm railroad station each night to buy copies of the newspapers *Kurier* and *Tidning,* both published in the provincial city of Karlskoga, where munitions are manufactured.

[Codebreakers 373.jpg]

*A sheet of a one-time pad captured on Communist spies in Japan, 1961. One side may be for enciphering, the other for deciphering.*

Studying the papers, police noticed a number of oddly worded announcements. When they inserted similar advertisements, using the

same identifying words, they received responses from several people who turned out to be Red agents. Eventually a ring that operated in five cities was broken up and four Communist satellite diplomats declared persona non grata.

The most catastrophic instance of the eggshell ciphers of local Communists took place in Iran. On the night of

August 16, 1954, Iranian security police arrested Ali Ab-basi, a former Army captain who had come under suspicion because of his activities in the Red Tudeh party. In the suitcase he was carrying as he came out of a house in Teheran, they found a complete plan of Shah Mohammed Reza Pahlevi's summer palace, showing guard posts and the number of men stationed at each, top-secret documents from Army files, reports on the disposition of artillery along Iran's Russian border, two notebooks in what were obviously cipher, and another with page after page of what appeared to be trigonometric equations, replete with the Greek letters beloved of mathematicians and the abbreviations for "secant," "cosine," "tangent," and "cotangent." The problem was that mathematically the formulas made no sense at all.

Colonel Mostafa Amjadi, chief of the intelligence directorate of the Teheran military governate, and another colonel in the Iranian Army went to work on the three notebooks. By August 30, they had cracked the two overt codes, but extracted only meager information from them. Meanwhile, Abbasi decided to talk. He revealed that the Tudeh party had riddled the Iranian Army with about 400 agents and that their names were listed in a mathematical cipher. This was the trigonometric system which Amjadi and his colleague were even then struggling with, but Abbasi warned that the system was so complex that it could be read only by its inventor, Lieutenant Colonel Jamsheed Mobasheri, an artillery officer regarded by his friends as something of a mathematical genius.

Mobasheri was picked up for questioning. Instead of revealing the key, he tried to puncture a vein with a rusty nail. The two colonel-cryptanalysts worked steadily 24 hours a day in overlapping shifts of 12 hours each. Mobasheri was again interrogated, and, now that the first shock of arrest had worn off, his pride of authorship in his cipher almost overcame his loyalty to Communism and he twice agreed to reveal the method—only to change his mind both times. The Iranian government quietly asked other countries if they would help in the solution. Meanwhile, one of the colonels formulated a theory as to Mobasheri's system and interviewed him, hoping to get some clues from the inventor's reactions.

[Codebreakers 375.jpg]

*The imitation "trigonometric" cipher of red agents in Iran*

Mobasheri stubbornly insisted that the system could not be broken, but just as the colonel was leaving the cell Mobasheri's appreciation for an intelligent analysis broke through, and he admitted that the cryptanalyst was on the right track. On September 3, as an airplane was

about to fly copies of the trigonometric notebook to an ally's cryptanalysts, the two haggard colonels cracked Mobasheri's cipher.

The roster proved to be as detailed as an official army register in describing the officers, making identification easy. But it was so extensive that it took several days to decrypt it and locate the conspirators. A week later all 400 were arrested. This enormous conspiracy, Iranian security

police discovered, had not only obtained detailed information on the strength and disposition of Iran's entire armed forces, but had wormed into vital posts that would have enabled it to assassinate on a moment's notice members of the government from the Shah on down. It was ready either to pull a coup and set up its own Communist puppet government or to deliver the nation entire to the Soviet Union. Imperfect ciphers kept it from doing either. Instead, 26 of its leaders—including Mobasheri—were executed, and hundreds of run-of-the-mill plotters and sympathizers were jailed. A poisonous infection had been cleaned out; a year later Iran abandoned her traditional neutrality and, signing the Baghdad Pact, aligned herself with the West.

No cryptographic weakness imperils the operation of Russian spy rings. Perhaps the most striking example lies in the cipher used by Abel's lieutenant, Reino Hayhanen.

The system dispensed with written keys such as Abel's one-time pad, which helped incriminate him. Hayhanen had to remember only four basic keys—SNEGOPA(D), the first 20 letters of a Russian popular song ("The Lone Accordion"), the date of the World War II victory over Japan (3/9/1945, in the Continental style), and his personal keynumber (13, changed to 20 in 1956). The latter three keys generated the keys for two transpositions and the coordinates of a straddling checkerboard through a process that was complicated but that possessed a kind of tractive logic, was meant to be memorized, and probably would be after two or three run-throughs.

This process injected an arbitrary five-digit number at the very beginning of the key derivation, strongly influencing the end result. (This number was also inserted in a predetermined position in the cryptogram so that the decipherer would have it. In Hayhanen's case, this position was the fifth group from the end, the position coming from the last figure, 5, of the victory date.) This group changed from message to message, so the enciphering keys, and consequently the ciphertexts of all messages enciphered in this system, would bear no exploitable relation to one another. Not only would the transposition keys differ, the very widths of the blocks would as well—this being a variable stemming from the key derivation. This kills any last hope of an analysis by comparing messages. The poor cryptanalyst would even be denied the consolation of discovering a common origin of the cryptograms through

similarities in frequency counts, for the coordinates themselves would change. Any solution would thus have to be effected on the basis of a single message. It would require trying every sensible pattern of transposition until one was found that yielded a monoalphabetic frequency count of the digits. A complication greatly increases the difficulty of finding this pattern, just as the straddling effect increases the difficulty of getting a valid frequency count. The number of trials for a 1,035-digit message like a Hayhanen one is astronomical, and, even with computers, it would probably take years. In theory the system is not unbreakable, but in practice it is. Its security could not have been more pointedly demonstrated than by the F.B.I.'s failure to solve it.

Such is the cryptology of the Soviet Union. It is interesting to contemplate its excellence. Russia herself remains "a riddle wrapped in a mystery inside an enigma." So, when she decrees it, do her communications. The one-time pad ensures this for the bulk of her spy messages and for a fair proportion of her diplomatic and secret-police mes-ages. Complex rotor-type cipher machines, well-designed in themselves and handled with a sophistication that changes keys after foreign cryptanalysts have reconstructed part of the wiring and the rotation pattern but before they can read any plaintext, guard other high-level diplomatic and military messages of Soviet Russia. And even when she requires a cipher to be fully mnemonic, like Hayhanen's, she designs it so that it cannot be broken. She has solved, during the Cold War, ciphers in use at the American embassy in Moscow. Feats like these bear witness to knowledge that could only well up from a profound understanding of cryptography and cryptanalysis. Whether this comprehension springs from the scientific ability that has enabled Russia to orbit great artificial satellites, or from the decades-long experience of cryptology that the Communist dictators have had to practice for self-preservation and aggrandizement, or from the habits of secrecy and puzzling out the real meaning of things that are ingrained into every inhabitant of a totalitarian society, or from a dark-souled Slavic love of the mysterious, it has beyond question rocketed Red accomplishments in this black art to Sputnik height.

.

## 17. N. S. A.

IT HAS BEEN said that 90 per cent of all the scientists who have ever lived are living today. The remark applies to cryptology with even greater force. The age is one of communications and of Cold War. The titans that confront one another in Berlin and Vietnam and outer space owe much of their effectiveness as superpowers to the vast webs of communications through which they receive information and transmit commands. These networks, more extensive and more heavily used than any in history, furnish cryptologists with unparalleled opportunities. The Cold War gives them the impetus to exploit these opportunities —a stimulus that, in view of the dangers of national extinction, becomes almost an imperative. These two factors converge to produce more cryptology and more cryptologists than ever before.

Even considering only the radio circuits, the possibilities for traffic analysis and cryptanalysis are enormous. The United States protects itself from these, and at the same time it exploits the opportunities afforded by the comparable Communist networks. The hugeness of this task has engendered the greatest cryptologic organization in history—the National Security Agency and the three armed service cryptologic agencies.

N.S.A. probably owes its existence, like the Central Intelligence Agency and the Department of Defense itself, to Pearl Harbor. Congress, after its investigation of the surprise attack, recommended "that there be a complete integration of Army and Navy intelligence agencies," and the record of the investigation contains a few anticipatory suggestions for cryptologic centralization as well. Major General C. A. Willoughby, MacArthur's G-2, complaining about Navy selection of cryptanalyzed information passed over to him, admonished: "The solution to this vexing and dangerous problem is a completely joint, interlocking intercept and cryptoanalytical service, on the highest level, with the freest interchange of messages and interpretation." 378

| | N.
S. A. 379

*%:* Colonel Henry Clausen, who investigated MAGIC in 1944, told the Joint Congressional Committee the following year: *- "I also think that the basic recommendation that can come *L* from this committee is a very fine one if you make it that f never again shall MAGIC, this information, be monopolized ; by one service or the other service, but have it distributed *".-..* by one agency on an overall basis." Former Pacific Fleet y intelligence officer Captain Edwin Layton may have had this in mind when, after deploring the publicity given to American cryptanalysis by the committee probe, he added that "it may serve a very fine purpose for the future." And in a memorandum concerning a proposed Central Intelligence Agency that Allen W. Dulles submitted to the Senate Armed Services Committee in 1947, the future Director of Central Intelligence noted that "An important balance [to intelligence obtained openly] must be supplied by secret intelligence which includes what we now often refer to as 'Magic,' " and that any Central Intelligence "t-;'~ Agency should have access to "intelligence gained through !',. intercepted messages, open and deciphered alike."

In the first postwar years, the cryptologic duties of the j' American armed forces reposed in the separate agencies of the Army, the Navy, and the Air Force. The Army, at I, least, charged its agency with maintaining "liaison with "{ the Department of the Navy, Department of the Air I Force, and other appropriate agencies, for the purpose of t| coordinating communication security and communication S intelligence equipment and procedures." Presumably the * Navy and the Air Force units were similarly charged. This |: arrangement, which relied on internal desire instead of jj external direction, prolonged the abuses hinted at by Wil-I loughby. To rectify them and achieve the benefits of I centralized control, the Defense Department in 1949 established the Armed Forces Security Agency. The I A.F.S.A. took over the strategic communications-intelli-*1* gence functions and the coordination responsibilities of the individual agencies. It left them with tactical communica-£ tions intelligence, which can best be performed near the point of combat and not at a central location (except for basic system solutions), and with low-echelon communications security, which differs radically in ground, sea, and air forces. Even in these areas A.F.S.A. backed them up. A.F.S.A. drew its personnel from the separate departmental

agencies, though it later hired separately, and housed itself in their buildings.

The merits of the unified approach to cryptology quickly manifested themselves. They warranted expanding that approach beyond the Defense Department to all cryptologic activities of the United States government, such as State Department cryptosystems. Accordingly, President Harry S Truman promulgated a directive that created the National Security Agency on November 4, 1952, abolishing A.F.S.A. and transferring its personnel and assets to N.S.A.

That directive was classified as security information, and for several years no government document publicly acknowledged the agency's existence. Finally, in 1957, the *United States Government Organization Manual* included a brief but vague description. Today the official description reads:

> CREATION AND AUTHORITY.—The National Security Agency was established by Presidential directive in 1952 as a separately organized agency within the Department of Defense under the direction, authority, and control of the Secretary of Defense who was designated executive agent for the performance of highly specialized technical functions in support of the intelligence activities of the United States.
>
> PURPOSE.—The National Security Agency has two primary missions—a security mission and an intelligence information mission. To accomplish these missions, the Director, National Security Agency, has been assigned responsibilities as follows: (1) prescribing certain security principles, doctrines, and procedures for the U.S. Government; (2) organizing, operating, and managing certain activities and facilities for the production of intelligence information; (3) organizing and coordinating the research and engineering activities of the U.S. Government which are in support of the Agency's assigned functions; and (4) regulating certain communications in support of Agency missions.

The unspecified nature of those two missions involves, of course, cryptology. In its security function, N.S.A. creates

IN. 5. A.

381

and supervises the cryptography of all U.S. government agencies. In intelligence, it intercepts, traffic-analyzes, and cryptanalyzes the messages of all other nations, friend as well as foe.

In its first years, A.F.S.A.-N.S.A. was scattered in offices throughout the Washington area, notably at Arlington Hall, home of the Army Security Agency, though its official address was 3801 Nebraska Avenue, North West, home of the Navy branch. In 1953, however, the Defense Department called for bids on the preliminaries for constructing a single big building at Fort George G. Meade, Maryland, about half way between Washington and Baltimore. In July of 1954, the Charles H. Tompkins Company of Washington was awarded a $19,944,451 contract to construct one of the most costly buildings in the Washington area on an 82-acre site in conjunction with the J. A. Jones Company. It was essentially completed in the fall of 1957, but it was not until early in 1958 that the last of the employees had moved in. By then the total cost had risen to about $35,000,000 for the structure, for associated facilities such as parking lots, utility lines, electrical power substation, supply building, and barracks for the Marine Corps guards, and for moving in existing equipment and installing new.

The long, three-story structure, of concrete, glass, and steel, in the shape of a squared-off A, stands in a shallow bowl fringed with pine trees and surrounded by acres of asphalt parking lots. It faces south, fronting upon Savage Road, a narrow road that widens as it passes N.S.A. and then shrinks again. The Baltimore-Washington Expressway runs a few hundred yards to the west. This Operations Building is 980 feet wide by 560 feet deep, and along its full width runs the longest unobstructed corridor in the country, an honor previously claimed by the 750-foot central corridor of the United States Capitol.

In addition to dozens of offices and basement facilities for computers, the structure encloses a cafeteria accommodating 1,400 and an auditorium seating 500, eight snack bars, a post exchange, a dispensary with X-ray and operating rooms and dental chairs, a shoe-repair and clothes-cleaning shop, a barber shop, and a branch of the State Bank of Laurel. A system of "security conveyor belts" runs through the basement, carrying trays of documents to eight substations. A German pneumatic-tube system can whisk

up to 800 containers an hour at 75 feet per second to interoffice destinations selected by a dial at each station. The building is fully air-conditioned. It has a public-address system. It is said to have more electric wiring than any building in the world. Its institutional, characterless offices, filled with metal desks, partitions, and lockable file cabinets, are the black chambers of today.

But although this cathedral of cryptology—far and away the greatest ever erected to that science—was the third largest building in the Washington area (after the Pentagon and the new State Department headquarters), and although its 1,400,000 square feet exceeded the C.I.A.'s 1,135,000, it proved too small after only five years. In May of 1963 the J. W. Bateson Co., Inc., was awarded a contract for $10,940,000 to construct a nine-story Operations Building Annex of boxy, modern style between the jutting arms of the square A. It added 500,000 square feet to the N.S.A. headquarters complex, 140,000 of it in a basement area almost certain to be used for computers. The annex was completed in late 1965.

This expansion was clearly made necessary by the rapid growth of the agency. In 1956, the director told a Senate committee, "We have almost 9,000 civilian employees here in the Washington area and around the world." In 1960, two former employees reported that 10,000 persons worked in the Operations Building. Based on a nationwide governmental average space-utilization of 150 square feet per worker, the two N.S.A. buildings would house more than 12,500 employees; based on the figure of 135 square feet per worker that modern buildings attain, the number of employees there would exceed 14,000. This is certainly greater than the number of C.I.A. employees in Washington, estimated at about 10,000, and even when the uncertain numbers of employees of both agencies in posts around the world are added to their totals, N.S.A. is still larger than C.I.A., making it almost certainly the largest intelligence agency in the free world. (At least a thousand N.S.A. employees are stationed overseas. Several hundred work in each of two branches, N.S.A. Far East in lapan and N.S.A. Europe in Germany. Others serve with N.S.A.'s worldwide intercept net, a few as radio operators, most as supervisors, since nearly all the intercept operators are armed forces personnel.) N.S.A.'s budget has also been reported to be twice as large as the C.I.A.'s.

The presidential directive that created the National Security Agency was and is classified as security information, and the veil thus thrown around the agency at its very birth has cloaked it to this day. N.S.A. is even more still, more secret, and more grave than the C.I.A., whose basic functions are set forth in the 1947 law that created it. C.I.A. officials have occasionally issued statements to the press and have more often leaked favorable publicity. N.S.A. officials never have. The National Security Agency thus remains the most reticent and least known organ of the entire hush-hush American intelligence community.

At N.S.A. security begins outside. Three fences ring the headquarters building. The inner and outer are Cyclone fences topped with V's of barbed wire. The middle one is a five-strand electrified wire. These are pierced by four gatehouses manned by Marine guards. When the gates are closed, a complicated electronic apparatus involving mirrors and lights buzzes warningly. Gatehouse 3, on the north side of the building, is open 24 hours a day.

Security permeates N.S.A.'s interior as well. Both the agency's organization and the physical arrangements that reflect this organization are highly compartmented, with numerous checkpoints, and employees are not permitted to enter areas in which they do not work without special permission. Colored badges limit them to their own areas. Pistol-packing guards block the entrance to specially restricted areas. The most secret documents must be locked in three-tumbler safes except when analysts are actually working on them—and these areas are also patrolled night and day. Offices that generate the least confidential documents in quantity may store them in desks or in file cabinets, sometimes unlocked, but these offices are under constant armed guard. When classified papers must be taken from N.S.A. to other agencies, employees must not go alone if they use a private car but must travel in pairs. They must keep the papers in a locked briefcase and must store them overnight in a safe stowage either at the other agency or at N.S.A.; they may not take them home.

Among the agency's deep secrets is its annual budget. N.S.A. does not appear in the federal budget. All its funds, like those of the C.I.A., are cunningly concealed by adding a few million dollars to each of several line items in other parts of the budget. The chiefs of the agencies whose budget figures are thus padded know only that the money

is for a classified project, but in many cases Congress is told in executive sessions what the figures are for these projects. The Secretary of Defense can legally shift the funds from one unit to another, within certain limits. Unlike the C.I.A., N.S.A. finances are audited by the Government Accounting Office. The results, however, have not been shown to Congress, G.A.O.'s boss.

The employees themselves must pass the strictest security standards in the Department of Defense. A prospective employee must pass the National Agency Check, in which several investigative agencies report any facts they have bearing on his loyalty. He must also pass a lie detector test. * He may then be hired for training, but final clearance depends upon a full Background Investigation. This involves verification of birth, education, and employment records, interviews with friends, neighbors, and former co-workers and employers on.his trustworthiness and maturity, analysis of credit records, and a further check for membership in subversive organizations. No one who has close kin in an Iron Curtain country may be hired. Even after having passed these requirements and been hired, all employees undergo follow-up checks every four years to make sure that their security clearance should be maintained. All except some of the older employees must pass repeated lie detector tests. They must also periodically sign a certificate that they have read Public Law 513.

N.S.A. dins security security security security into its employees with remorseless persistence until it becomes more than habitual, more than second nature—it becomes virtual instinct. Many, perhaps most, N.S.A.ers never tell their wives and children just what their jobs are. "N.S.A.," they explain, stands for "Never Say Anything." The Security Education Program pulls out all stops: "Our job with N.S.A. is essential to the preservation of our American way of life. As part of that job, fulfilling our security obligations is equally essential to the success or failure of this Agency in the accomplishment of its mission." So thorough is the indoctrination that one employee wondered in a poem whether being not allowed to say what he did in this world would have dire effects in the next:

*This has led to abuses. One 17-year-old girl, trying to get a job as clerk-typist with N.S.A., was asked many over-intimate questions about her sex life.

But to St. Peter, must I say,
"I learned my lesson well.
You see, I worked at N.S.A.,
So send me on to------."

The cutting edge of cryptologic progress in the United States is N.S.A.'s Office of Research and Development, or R/D. Solomon Kullback, one of the three cryptanalysts that Friedman hired in 1931, served as its head in the early 1950s. In 1957, Howard H. Campaigne, a Ph.D. in ^mathematics specializing in statistics and hypergroups, be-?came head of the mathematical section at the age of 47. -His assistant is Dr. Walter W. Jacobs, a mathematical ; statistician who had previously served in the Office of Production.

R/D is divided into three sections called REMP, STED, and RADE. REMP—the term stands for "Research, Engineering, Mathematics, Physics"—conducts basic cryptanalytical research. It ransacks the domains of statistics and higher algebra for ever more sensitive and more powerful tests to solve complex ciphers. It attacks difficult foreign crypto-systems to devise new techniques of solution; any intelligence obtained is, so far as R/D is concerned, a by-product of this search. It advises other N.S.A. divisions on problems involving new methods. It works intensively to improve computer applications to cryptology. Engineers and physicists seek increases in computer speed and data-handling capacity by transistor circuitry, short-pulse techniques, time-sharing, and magnetic memories. A recent effort involved eliminating speed-inhibiting factors from such memories. REMP uses computers to design computers, and engineers working on peripheral components, such as line printers and punched-card inputs, must strain to keep up with basic technology. N.S.A. leads even such firms as I.B.M. and Remington Rand in important areas of computer development, such as time-sharing, and industry has adopted many N.S.A.-designed features.

The second section, STED (for "Standard Technical Equipment Development") conducts basic cryptographic research. It looks for new principles of encipherment. It ascertains whether new developments in technology, such as the transistor and the tunnel diode, have cryptographic applications. Using such esoteric tools as Galois field theory, stochastic processes, and group, matrix, and number theory,

machine and will simulate its operation on a computer, thus producing the cipher without having to build the hardware. Rotor principles have often been tested for cryptographic strength in this way. It devises audio scramblers, from the ultra-secure types for high officials to the walkie-talkies of platoon commanders, as well as video scramblers for reconnaissance television and for facsimile. Their development involves sciences from metallurgy to optics, as well as techniques—important in miniaturization—from printed circuits to ferro-resonance.

R/D's third section, RADE (for "Research And DEvelop-ment"), conducts basic transmission research, going deeply into such matters as the interaction of electromagnetic radiation and matter. It aims both at increasing the sensitivity of American intercepting receivers and the security of American transmission methods. N.S.A. radios operate at the extreme limits of radio frequencies and involve all types of electromagnetic emanations. Its listening posts require both panoramic receivers to scan the entire frequency spectrum and single-frequency receivers with a high degree of stability that will not drift off a signal. RADE strives constantly for antenna arrays that will accentuate the signal and eliminate atmospheric interference and circuit noise so as to pick up even the weakest radio messages. It improves direction-finding apparatus and devises radio fingerprinting apparatus. And it looks into new techniques of communication, such as methods that spread a transmission over so broad a frequency spectrum that anyone listening on one frequency band would hear only a faint crackle like static. These may themselves afford some security—at least until the enemy's technology catches up. Presumably it is investigating the possibility of sending messages by laser.

In addition, N.S.A. engages in some basic communications research in the broadest possible sense. The flow of impulses through a computer's circuits constitutes a study in communication, and N.S.A. mathematicians investigate it. They use the tools of the new field of information theory to look into other problems—compression of maximum information into a minimum bandwidth, expected percentages of errors, rates of transmission, pattern recognition. N.S.A. physicists study modern quantum theory of many-body systems, superconductivity, magnetic resonance,

the electromagnetic properties of solids, and the scattering effect of the ionized region of the troposphere for possible application to communications. Language itself is dissected phonetically, phonemically, grammatically, logically, se-mantically, historically, statistically, and comparatively. These studies result in one of N.S.A.'s few unrestricted products: dictionaries and grammars of more recondite tongues, such as the 429-page *Vietnamese-English Vocabulary* issued by the Office of Training Services, the *Romanian-English Dictionary,* prepared by N.S.A.'s 762 Dictionary Unit, and *A Grammar of the Bulgarian Language.* R/D's research differs from that carried out by the Institute for Defense Analyses' Communication Research Division at Princeton in generally being rather more applied in nature. I.D.A. research is freer, more "far out."

Smallest of N.S.A.'s three operating divisions—and the only one whose duties are publicly acknowledged—is the Office of Communications Security, or COMSEC. It is responsible for the protection of secret American government communications. Consequently it prescribes or approves the systems each department must use and how they must use them. It furnishes some machines itself and lets contracts for the others. It promulgates the national crypto-security doctrine and supervises its execution.

"All cryptographic material (including cryptographic equipment, instructions, spare parts, and associated materials for the Armed Forces) is produced by, or procured under, the direction of N.S.A.," states an Air Force manual. The same must be true for the Army, the Navy, and the State Department. COMSEC standardizes as much of American cryptography as practicable, down to the short titles of communications security publications. Thus the Air Force Communications Security Manual 2, formerly known as AFCOMSECM-2, is now listed as AFKAG-2. COMSEC prepares courses of instruction for new cryptographic equipment and issues regulations for its operation, presumably mandating such matters as the when and how of primary and secondary key changes. For interdepartmental and presidential communications, it probably produces the keys—rotor wirings, lists of positions, one-time tapes. Keys for communications wholly within, say, the Air Force are presumably produced by its own cryptographic agencies.

COMSEC, drawing upon R/D's STED, devises new systems

of encipherment and embodies them in new mechanisms. It works closely with potential users, such as the State Department, to make sure that the equipment fits the user's needs and at the same time provides adequate security. COMSEC engineers test this equipment for reliability in vibration machines and salt-spray chambers. They assure its compatibility with the user's existing equipment, and they cooperate with the manufacturer to get the best devices at the lowest cost.

In addition to the suggestion that contractors make for improving machines, COMSEC evaluates the hundreds of ideas for new "unbreakable" cipher systems that pour in upon the National Security Agency from amateur cryptographers. The agency gets at least one a day, often channeled to it from the Army or the F.B.I, or the State Department. Many are from professional men, such as doctors and lawyers, but one came in from a prisoner (it was forwarded by his warden). A good percentage include a challenge message, and the COMSEC experts can just visualize the devilish grin of the inventor as he finishes enciphering the message, and thinks, "They'll never get *that!"*

The inventors fall into two categories. One type has just read Edgar Allan Poe's dictum in "The Gold-Bug" that "it may well be doubted whether human ingenuity can construct an enigma of the kind which human ingenuity may not, by proper application, resolve," and has, in half an hour, invented an unbreakable cipher that disproves it. The other has just devised a cipher so simple that a 12-year-old can operate it (never a 13-year-old), and as a patriotic American is giving it to his government for a mere $100,000—a cheap price for assuring the security of information worth much more than that.

Few of the inventors have any idea of the volume of modern communications, of the conditions under which ciphering is done, of modern cryptanalysis, or that the unbreakable cipher, in the form of the one-time pad, already exists. Nearly all the systems are pencil-and-paper, which are all but useless today, and the chances are almost nil that even a tinkerer in a machine shop will come up with anything new and worthwhile. Nevertheless, COMSEC looks seriously at every proposal. It perhaps recalls that all the basic cryptographic principles now in wide use—the rotor, the Jefferson cylinder-strip system, the one-time tape, the

Hagelin mechanism—were created by persons with no professional cryptologic background. The next letter may come from a new Hebern, submitting a valuable concept. Besides, it's fun to solve the challenge cryptograms—which COMSEC very often does, despite a brevity that would never be met with in practice.

In a way, however, the agency seems to take unfair advantage of these inventors. Their ideas disappear into the black maw of the N.S.A. and may even see service in American cryptography, but security prevents the inventor from ever knowing of this—and may enable the agency or its employees to utilize his ideas without compensation. Fear of this may keep some inventors from submitting potentially valuable ideas. The agency might attract more suggestions by a firm promise not to use ideas without payment; this might be of some value if the matter ever came to court. But the agency will not give such a promise. More incomprehensibly, it will not even say why it will not. It seems that here N.S.A. is being deliberately self-injurious.

COMSEC presides over a great variety of cryptosystems. The Army requires different methods for the differing needs of front-line, middle-echelon, and high-command communications. The Navy's needs may not vary quite so widely, but even it uses strip cipher for less important communications and rotor machines for more important ones. The Air Force probably uses small codes for its airborne communications and a host of systems for its ground communications, including those to the missile-launch centers.

Are American cryptosystems secure? Different agencies investigate this question in different ways. N.S.A. tests the theoretical limits of security of ciphers. For example, COMSEC mathematicians might calculate the maximum number of messages that could be sent with unchanged primary key (as the wiring in a set of rotors) before enough secondary-key overlaps could be expected to make solution likely. They use such information to prescribe key changes. The individual agencies probably test the practical security of their own systems by monitoring and actual cryptanalysis; the State Department, for example, employs half a dozen cryptanalysts. In addition, independent tests [a]re made, as by the Institute for Defense Analyses. In one case, I.D.A. cryptanalysts were given 1,000,000 letters of

error-free text in a top military cryptosystem. They put in the equivalent of six man-years on it—and finally gave up in defeat. The episode speaks well for the security of that cipher, and, by implication, for that of other American cryptosystems.

Far and away the largest of N.S.A.'s three operating branches is the Office of Production, or PROD, with a little more than half of N.S.A.'s entire headquarters personnel. What PROD produces is communications intelligence. The term must be taken in the broadest possible sense. For although it includes cryptanalysis, traffic analysis, and analysis of cleartext traffic, it is not confined to studies of man talking to man. Communications intelligence in the Cold War includes machines talking to machines—the self-interrogations of radars, the remote-control systems of guided missiles, the telemetry of artificial satellites, the I.F.F. or identification-friend-or-foe systems. All these are communications devices, usually radios modified in one way or another, and a great deal can be learned from their location and operation. N.S.A. entered this electronic field in the 1950s, and began monitoring Soviet missiles in 1958, the year after Sputnik, largely due to the initiative of PROD'S Joseph P. Burke, a former traffic analyst.

PROD is always headed by a military man. The deputy at one time was Abraham Sinkov, one of Friedman's original three assistants. For many years the office was divided into eight sections. Four handled cryptanalysis and associated traffic analysis. ADVA (for "ADVAnced") attacked high-level Soviet cipher systems and diplomatic codes. GENS (for "GENeral Soviet") attacked Soviet military code systems and medium-level ciphers; its chief at one time was Francis A. Raven, who recovered the key-pattern of the Japanese PURPLE machine in 1941. ACOM ("Asian COM-munist") attacked the code and cipher systems of those nations, and ALLO ("ALL Others") attacked the cryptosystems of neutrals, Communist satellites, and the nations of the free world. A section called MPRO ("Machine PROcessing") provided computer services to the crypt-analysts. The section called Communications handled the intercept organization. The two other sections may have analyzed cleartext intercepts and studied the electronic material.

After W. H. Martin and B. F. Mitchell exposed this

arrangement, however, PROD was reorganized into three big sections. These were set up on a geographical basis, and each analyzes all communications within its area, from human cleartext to coded mechanical "messages."

To gather the raw material for these sections, N.S.A. and the armed forces have cast a fine-meshed net over the world of electrical communications. Around the globe they have spotted more than 2,000 intercept positions (one man listening at one radio set). Most are on U.S. military bases overseas, but some are on planes or aboard ship. More than 8,000 soldiers, sailors, and airmen, accompanied and supervised by N.S.A. personnel, type out on four-ply paper the Morse code messages that peep incessantly in their earphones. Other personnel tend the equipment that intercepts radioteletype messages and the tape-recorders for voice communications. Still others forward the intercepts to Fort Meade. Interception goes on around the clock, at every wavelength, for every audible transmission, of every single country.

Not all the human communications that N.S.A. studies are coded. Into the headquarters building at Fort Meade come recordings of the cleartext chatter between Soviet pilots. An N.S.A. section transcribes these, not into ordinary Russian writing, but into a phonetic representation that retains the pronunciation variations of the speakers. These transcription sheets go to analysts in another section. They compare the pilots' inflections with known dialectical pronunciations to determine where the men in a squadron come from. Long residence in one locality will sometimes shade an older pronunciation more toward the local one; the analysts can detect this and tell where the squadron is stationed. Slang and current phraseology assists in these determinations. When one pilot calls another "Ivan," and Ivan replies, the characteristics of his speech are carefully noted in an enormous file with all other Ivans so that future clues can be fitted into the original ones to add more details. lokes, comments about superior officers, references to nearby units, remarks about the planes, all are catalogued. Sometimes an analyst will spend days on a single sentence, checking and cross-checking names and intonations. And just as the tens of thousands of points of pure color that George Seurat dabbed individually onto his canvas combined into the huge and stately "Sunday on

tne Grand Jatte," so the thousands of details elucidated by the analysts build up into a broad image of Soviet air power, fuzzier than the painting, of course, but with a great deal of collateral intelligence on capability, morale, equipment, and almost every subject which a potential adversary might find of interest.

But the National Security Agency produces its most valuable intelligence by breaking foreign codes and ciphers. And though "practical cryptanalysis" sometimes helps, most of the results come from true cryptanalysis. As Martin and Mitchell said: "Successes obtained by the National Security Agency in reading the code and cipher systems of other nations are due primarily to the skillfulness of crypt-analysts, frequently aided by electronic digital computers." Who are the cryptanalysts, and how many does N.S.A. have? It is difficult to give an exact answer, because modern cryptanalysis is so specialized and so subdivided that many N.S.A. employees engage in partial or elementary cryptanalysis, or do the nearly mechanical task of filling in the holes after the "real" cryptanalysts have made the entry into a code or cipher and have thoroughly broken it. However, a rough guess might place the number of "real" cryptanalysts in N.S.A.—those who attack unknown or new systems—at about 200.

Despite the great secrecy surrounding their work, and the great events that can flow from it, the cryptanalysts' labors resemble those of any other office workers. At N.S.A., they arrive in one of three shifts, beginning at 7:20, 7:40, or 8:00 a.m. (and ending respectively at 3:50, 4:10, and 4:30 p.m.). Once in, the first order of business must be to finish reading the newspaper and shoot the breeze with one's officemates. When they get down to work, they write on cross-ruled paper with colored pencils, shuffle pages, look for significant patterns, look for plaintext, confer with colleagues, take coffee breaks. Sometimes a yelp of joy will pierce the concentration as a cryptanalyst breaks through. They have one advantage at least over workers in more ordinary fields: they cannot take their work home with them at night. But, in another sense, they cannot get away from it, for a problem in cryptanalysis grips the mind, teases and torments it more than other problems, and never seems to let go. If an idea occurs at home, the cryptanalyst may write a note to himself, or, if he lives close enough, he

might perhaps drive down to the headquarters building to work on it.

As in other large white-collar organizations, they probably work in large open offices. Into them come the raw intercepts—no doubt, in most cases, the typewritten copies as made on four-ply paper by the intercept operators. Urgent messages are most likely forwarded by radio, as the MAGIC intercepts were sent to Washington from the Philippines. If several versions of the same message, picked up by several intercept operators, reach Fort Meade, editors will try to clear any garbles. Presumably traffic analysts then collate and compare sender location, routings, and indicators. This enables them to sort the messages into families of identical cipher systems for the cryptanalysts. And by studying traffic patterns, they can deduce tables of military organization and perhaps other information as well.

The cryptanalysts work in teams. Complex modern ciphers have rendered individual work as much a thing of the past in cryptanalysis as in other branches of science. Thirty-three atomic physicists signed the report announcing the discovery of the omega-minus particle; seemingly as many N.S.A. cryptanalysts would deserve credit for solving the rotor system of a sophisticated modern nation.

The head of the team apparently parcels out such assignments as different statistical tests, calls conferences, decides whether one attack is proving more fruitful than another. The cryptanalysts' work consists in essence of looking for textual patterns that deviate significantly from what could be expected by chance. These patterns are extremely tenuous, and the individual letters of which they are composed recur only at extremely long intervals. This results from the efforts of rotor systems, Hagelin machines, and computer-generated keys to make it as hard as possible for the cryptanalyst to assemble the monoalphabetically enciphered letters that he must have to reach a solution. Only enormous quantities of text can make these faint patterns visible, and only huge data-processing computers can engorge the rivers of letters and test the innumerable possibilities to solve the system in real time, which is to say before it has lost its usefulness. For computer processing, key-punch operators very likely punch the messages on cards, and technicians feed the cards into the computers.

N.S.A. probably has more computer equipment than any

other installation in the world. Some of those it reportedly has are general-purpose computers, such as the I.B.M. Stretch, one of the world's fastest and most powerful computers, the $2,898,000 I.B.M. 7090, which can perform 229,000 additions per second, and late-model Univacs; there is also the Atlas, which N.S.A. had built to its own specifications early in the 1950s, and probably several smaller general-purpose computers. The agency also has a great deal of special computer equipment. For example, a device may be built to run the kappa test instead of wasting a general-purpose computer on so restricted a task. N.S.A. may use its computers to determine which configuration of possible displacements on a rotor produces the group of letters that most closely resembles plaintext. The giant calculators may solve or partially solve the equations of group theory needed in analyzing a rotor machine. They may run test decipherments, simulating rotors wired in various ways and turning in various periods, and print out the test solutions at rates up to 600 lines per minute, starring those solutions that statistically most resemble plaintext. Undoubtedly the agency has prepared and debugged programs for common routines and holds them in readiness for immediate' use.

The computer has in no way conferred total victory upon cryptanalysis in its unending struggle with cryptography, for cryptography has kept pace with countervailing developments of its own. Nor has the computer automated the cryptanalyst out of a job. The computer has relieved him of much drudgery, but modern cryptosystems involve much more work than older ciphers. Computers could be programmed to recognize plaintext by stocking their memories with letter frequencies, 10,000 common words, and basic grammatical rules. But it could not do so as quickly as a human being. Furthermore, the computer would have to run through all of even the better possibilities in a modified "brute-force" attack—something which would take impossibly long. A human being can correct and enlarge partial solutions. And there is no machine yet devised that can, as quickly as the living computer inside the skull, make an inspired guess on the basis of a half-forgotten news item in the *Washington Post* of a month ago and last night's television news that the formless mess of letters *i-go-e-ia* must be a garbled *Indonesia.* Finally, and above all, a human brain must decide which tests the computer

should run on a sheaf of cryptograms. Cryptanalysis still has room—indeed, may have more room than ever before —for flair, intuition, experience, individual brilliance. The computers at N.S.A. are—as they are wherever computers are used—the tools of their operators, not their replacements. They are robot cryptanalysts to a very limited degree. Thus, in the last half of the twentieth century, in the flowering of the computer age, cryptanalysis often comes down to exactly the same problem that four centuries earlier faced the West's first great cryptanalyst, Giovanni Soro of Venice: Does x stand for *a* or o?

The quality of the systems N.S.A. attacks varies greatly from country to country. Competence in cryptology, as in other fields of endeavor, seems to vary in direct proportion to the technological knowledge and the economic wealth of a country. On this basis, the United States probably has the most secure cryptosystems and the most informative communications intelligence in the world. Of the nations whose cryptograms N.S.A. attempts to solve, unquestionably the most sophisticated must be the Soviet Union, Great Britain, and France, probably in that order.

In all probability, N.S.A. attempts to solve all cryptosystems of all countries—at least in principle. But manpower and monetary limitations afflict N.S.A. like other agencies, and these and the incessant emergencies that must require pulling a cryptanalyst off his regular task make the ideal unattainable. Thus, though N.S.A. might want to attack, for example, the middle-echelon military -systems of a Near Eastern country, it might have to concentrate the cryptanalysts that would be assigned to it on a Russian system that could be expected to yield more valuable results. How long it will keep a team working upon a system probably depends upon the information it thinks it will obtain. The agency may well keep a team examining cryptograms in a given system for two or three years, even though it has had no success, in the hope that one of the cipher clerks may some day blunder and open the way to a solution. For in modern systems, properly used and with frequent key changes, a cryptographer's error is the cryptanalyst's only hope. And when nations will pay their code clerks only $60 a week, as Italy did in Washington in the 1960s, to await such errors may not be pointless.

In addition to the general cryptanalytic effort, N.S.A. may mount special attacks if one of its customers requests

it. The State Department, for example, may request such a solution in advance of a high-ranking official's visit to another country or before a major diplomatic conference.

N.S.A. cryptanalysts probably solve foreign cryptosys-tems in degrees of completeness that range from total reading of all messages in a given system, to fairly full solutions with a few questionable patches, to partial solutions with many holes, to solutions in which, say, one or two rotors of several have been reconstructed but no plaintext has been read, to an absolute blank. Solutions probably also vary in time: the cryptanalysts may read a complicated system for a few months, then lose out again in a change of key.

The solutions must go to organizations in the U.S. government that require that information—military details to the Defense Department, diplomatic to State, and so on. These, together with the C.I.A., must be N.S.A.'s chief customers. Probably each class of messages has a distribution list. Individual messages may well be read at meetings of the National Security Council and the U.S. Intelligence Board. During the Korean War, the White House itself reportedly called for solutions, even though some were fragmentary. Currently, the President sees the N.S.A. "Black Book" every morning, brought to him by his military aide.

What does it all consist of? How successful is N.S.A., and how valuable are its results?

It is likely that N.S.A. reads only a small minority of the total volume of intercepts sent it—perhaps under 10 per cent. In peacetime, encipherers can work more slowly and more accurately than in war—yet even in the wartime conditions of the Russian front, with a great volume of messages and unquestionably many more errors, Germany's Army Group North solved less than 30 per cent of Russian military cryptograms. Moreover, the N.S.A. intercept posts probably concentrate on messages in the highest priority systems, yet these must be the best systems and must often resist solution, thus lowering N.S.A.'s average.

Nevertheless, N.S.A. does solve enough cryptograms to produce information of great value to the nation. Two agency employees who defected to the Soviet Union, William H. Martin and Bernon F. Mitchell, delineated the extent of N.S.A. success. The agency, they said, solved the codes of more than 40 nations—or just about half of all that there were when they spoke. Asked which ones, Mar-

tin replied: "Italy, Turkey, France, Yugoslavia, the United Arab Republic, Indonesia, Uruguay—that's enough to give a general picture, I guess." This range is remarkable. France is one of the world's great powers and has a long and strong cryptologic tradition. It stands as an American ally in the free world, as do the other major European country (Italy), the small Latin American country (Uruguay), and the neighbor of Russia (Turkey). Indonesia and the U.A.R. are both important neutrals in the Cold War. Yugoslavia is a renegade Communist country. The two defectors would not say whether the United States reads Soviet messages. But the Soviet predilection for the one-time pad in diplomatic messages, and its known cryptologic sophistication, make it most unlikely, except by a lucky accident.

Another N.S.A. defector, Victor Norris Hamilton, filled in some details of the Martin-Mitchell outline:

> I was listed[x]as an expert on the Near East Sector in the office designated ALLO, which means "All other countries." This sector concerns itself with the U.A.R., Syria, Iraq, Lebanon, Jordan, Saudi Arabia, Yemen, Libya, Morocco, Tunisia, Turkey, Iran, Greece, and Ethiopia. The duties of my colleagues in ALLO included the study and breaking of military ciphers of these countries, and also the deciphering of all correspondence reaching their diplomatic representatives in any part of the world. . . . N.S.A. reads the ciphers of all these countries by applying cryptanalysis. . .
>
> I knew for a fact that the State Department and Defense Department systematically read, analyzed, and utilized in their own interests the enciphered correspondence between the U.A.R. embassies in Europe and the U.A.R. government in Cairo.
>
> For example, I had in my desk all the deciphered communications between Cairo and the U.A.R. Embassy in Moscow relating to the visit of the U.A.R. government mission to the U.S.S.R. in 1958 for the purpose of purchasing petroleum in the Soviet Union. N.S.A. sent all these communications to the State Department just as it continually sends it the deciphered instructions of the U.A.R. Ministry of Foreign Affairs to its embassy in Washington. . . .
>
> It is especially important to note that American

> authorities take advantage of the fact that the U.N. headquarters is located on American soil. Their highhandedness has reached the point where the enciphered instructions of the governments of the U.A.R., Iraq, Jordan, Lebanon, Turkey, and Greece to their missions to the U.N. General Assembly fall into the hands of the State Department before arriving at their proper address.

The intelligence that flows out of Fort Meade mingles with intelligence from many other sources to help high officials determine national policy and tactics within the framework of American goals. N.S.A. intelligence is not as voluminous as C.I.A.'s, a former top C.I.A. official has said, but it is of a higher grade. All intelligence is evaluated for credibility, and cryptanalyzed intelligence must nearly always get the highest rating (some messages may be dummies) because it comes straight from the mouths of the subjects themselves. N.S.A.'s intelligence covers the gamut of communications of modern nations, from the minutiae of legation routine to the secret instructions to ambassadors. Even at its most complete, however, it can illuminate but part of the intelligence picture. The solutions allude to persons and facts and basic policies half known or unknown to the interceptor; they presuppose a common knowledge not at his disposal; they do not include information exchanged by personal contact, letter, telephone. Most messages mean little standing alone; only context makes them comprehensible. Cryptanalysis thus complements other forms of intelligence, overt and covert, just as they complement it.

Perhaps it is the incompleteness of cryptanalytic intelligence that led to American officials' apparently disbelieving it at the time of the Suez crisis, despite its seemingly unimpeachable authenticity. Just after that crisis had passed its peak, George Wigg, a Labor Member of Parliament, told newspapermen that the United States had broken British, French, and Israeli codes and so had prior knowledge of plans for their invasion of Egypt at the end of October and beginning of November, 1956. Though he attributed the solution to the "United States Air Research and Development Command, Griffis Air Force Base, Rome, New York," Wigg's basic point seems to have been independently confirmed by C.I.A. chief Allen Dulles, who

wrote several years later of the Suez invasion: "Here intelligence was well alerted as to both the possibility and later the probability of the actions taken by Israel and then by Britain and France." Why, then, did the United States take no action? Dulles does not say, but Wigg thought "that the United States State Department knew from the middle of October what the French and the Israelis were planning to do. What I think they may have doubted was that the British Government would ever be so foolish as to get caught up in an adventure which was bound to end in disaster." Secretary of State John Foster Dulles said at the time: "We had no advance information of any kind." The later contradiction by his brother Allen suggests that this may be a cover-up for failure to act. Wigg, moreover, is not an M.P. whose inside information can be taken lightly: in 1963 he exposed the John Profumo-Christine Keeler scandal that very nearly toppled England's Conservative government. Suez has been called one of America's worst intelligence disasters. It seems more likely that the fault lay, not with the producers of intelligence, but with the consumers. No human being has ever had difficulty in finding an excuse to overlook an unpleasant fact. The consumers did not want to believe the contrary evidence of the cryptanalyzed intelligence (assuming that it existed). So they simply did not believe it—and perhaps justified their disbelief on the basis of its incompleteness. Against this human predilection no form of intelligence can prevail.

Yet where personal factors are less strongly engaged, cryptanalysis must assert *itself* as one of the most useful of intelligence sources. Its intermingling with other sources make it difficult to gauge its own particular value to the American government. The message that by itself leads to results as spectacular as those of a Zimmermann telegram or a Yamamoto flight schedule must be exceedingly rare. The impact of cryptanalysis must come in the way that the falling of many snowflakes, each one imperceptible to the ear, adds up to make an audible hiss in a wood.

Occasionally, however, instances occur in which the importance of cryptanalysis has been made manifest. One such case was Hamilton's referring to "the letter in which Henry Cabot Lodge, then the American ambassador to the United Nations, expressed his appreciation to members of ALLO for information about the instructions sent by the

Near East governments to their U.N. missions." Another— which showed the unsung workers at N.S.A. that the highest official in the land appreciates their work—came on March 2, 1966, when career cryptanalyst Frank B. Rowlett received the National Security Medal in a White House ceremony from the hands of the President of the United States himself.

Where, then, is the science headed? Are there any trends that can be foreseen? For there are fashions in cryptology as in other things. The one-time pad, very popular after World War II, has fallen out of favor. More popular now seem to he rotor machines—with from three to eight rotors —and Hagelin machines. For airplane and front-line messages, small codes seem to be common.

Future developments may be foreshadowed by a U.S. Air Force statement that

> One of the primary Air Force communications security objectives is total security of AIRCOMNET [the basic wire and radio teletype network] at the earliest date. It is intended to accomplish this by means of link encryption. This is a system which is integral to the communications system and which automatically secures all links of the communications system by on-line synchronous devices. When total security of AIRCOMNET is achieved, two distinct advantages will occur:
>
> (1) Unclassified common-user traffic introduced into AIRCOMNET will not be vulnerable to unfriendly intercept and analysis. U.S.A.F. Security Service has repeatedly revealed, through analysis of clear text unclassified traffic now being handled over AIRCOMNET, vital information regarding the Air Force order of battle, disposition and employment of combat air power, functions of key personnel, and similar data.
>
> (2) It will be possible to introduce classified messages up to and including SECRET into AIRCOMNET, without first resorting to off-line processing.

This is part of a more basic Air Force aim of a communications complex that will "provide full protection for information flowing within Air Force communications channels, including the exclusion of unauthorized entry

into the systems. This goal will be approached, first, by providing COMSEC protection to each of the individual communications networks and later by providing total end-to-end encryption throughout the complex."

The Air Force drive toward total end-to-end encipher-ment carries with it a tendency toward a single all-purpose cipher, for such encipherment can most easily and most safely be applied by such a cipher. A single all-purpose cipher, simple enough for the lowest echelon, secure enough for the highest, variable enough to nullify the danger of capture or compromise, would eliminate or reduce many of the problems produced by the present multiplicity of systems—the need sometimes to reencipher a message in a system the ultimate recipient holds, the difficulties of storing, distributing, and accounting for half a dozen different sets of ciphers instead of for just one.

One possible form of this ideal cipher—perhaps the most likely—is that of a system using a long, quasi-random key generated by mathematical methods and "added" to the plaintext, either numerically as with the one-time pad or electrically as with the Vernam method. A special-purpose computer might produce such a key from a few key digits, some of them common to the whole communications net and changing at fixed intervals, some chosen at random by the encipherer for each message and inserted at a prearranged place in the cryptogram.

Many generating methods are possible. The simplest is chain addition. Successive digits of the priming key are added together and the sum tacked onto the end of the keynumber, forming part of it, and the process repeated with these digits. For example, with the priming key 396 4, 3 and 9 are 12, which is listed as 2, since all addition is noncarrying and tens digits are dropped; 9 and 6 are 5, and

6 and 4 are 0. These three figures join the key at its tail: 3964250. The process is then continued with 4 and 2, making 6, which is put on after the 0, with 2 and 5, making a 7 which is put on after the 6, and so on: 39642506

7 5 6 3 2 1 .... More complex methods are possible. The computer might multiply a base keynumber for the day by a message keynumber to ten places, then multiply the product by the basic key to ten places, that product again by the basic key to ten places, and so on, each time extracting the last four digits of each product as the final key.

Modern algebraic techniques now enable the key generation system to be made so complex that, given a portion of the key, the rest of it cannot be projected forward to enable future messages to be deciphered. Small, special-purpose computers using electronic devices called shift registers can generate such keys in the form of digital pulses or numbers. Mechanisms like these serve American diplomatic purposes today and will undoubtedly come into increasing use as the cipher of the future. Thus cryptology would return in a more sophisticated way to a universal system, from which it has been divorced since the telegraph destroyed the nomenclator.

But what about the field as a whole? The growth of political cryptology has been exponential since it began 4,000 years ago. Will new methods like lasers, which provide hard-to-intercept line-of-sight communications, reverse that trend for the first time?

Probably not. Radio's advantage in establishing out-of-sight communication is so great that its use will probably continue to increase, just as communication and literacy itself always have. In any case, the advent of such techniques as the laser would merely shift the element of secrecy from cryptography to transmission security. It would not diminish the amount of secrecy in communication. Though in the past the amount of secrecy—the amount of cryptology, in other words—has always grown as rapidly as communication itself has, the secrecy comes not from the communication but from politics, from statecraft, from the governments who apply and seek to remove that secrecy. The future of cryptology contains many questions of technology, but the waxing or waning of the field as a whole is not among them. That question is human.

## 18. Heterogeneous Impulses

FEW FALSE IDEAS have more firmly gripped the minds of so many intelligent men than the one that, if they just tried, they could invent a cipher that no one could break. Many have tried and, although only a fraction of their

ciphers have been published or patented, the quantity and variety of even this small sample is astounding.

Emile Myzskowski, a retired French colonel, devised a kind of repeated-key transposition and published it in his *Cryptographic indechiftruble.* Collon, a Belgian Army officer, proposed a number of fractionating systems. One Rozier marched his plaintext letters through the interior of a Vigenere tableau in a dizzily twisting path in an attempt. to lose the cryptanalyst. The so-called Phillips cipher enciphers five letters monoalphabetically in a 5 X 5 square, then shifts the lines of the square and repeats the process. The Amsco transposition cipher acepts both single letters and pairs as its plaintext elements. A. de Grandpre filled a 10 X 10 square with ten 10-letter words whose first letters form a mnemonic acrostic, then ranged coordinates on the outside and used these to encipher; the use of plaintext words inside provides homophones in approximately the proportion required to disguise the frequencies of normal plaintext. A French major, Louis-Marie-Jules Schneider, concocted an enormously complex polyalpha-betic whose alphabets were generated one from the other; this was one of the systems William F. Friedman broke in evolving the principle of the index of coincidence. A mathematician named Arthur Porges devised a system based upon a continuing fraction. The Nicodemus cipher sets out a plaintext beneath a keyword, enciphers it in Vigenere according to that keyword, and then transposes it vertically by keynumbers derived from the keyword. The Count de Mirabeau, an 18th-century French revolutionist, enciphered in a Polybius square whose sets of coordinates both ran from 1 to 5; he wrote each two-digit equivalent vertically and then transcribed all of the first digits and then all of the second, inserting numbers from 6 to 0 at will as nulls. Some amateurs just propose enciphering a message in Vigenere and superenciphering the text in Playfair. There have been autokey transpositions and a cipher invented by W. B. Homan that produces a cryptogram in which every letter of the alphabet occurs as often as every other.

Beyond these pencil-and-paper systems, the files of the patent office bulge with quantities of cipher disks—probably the most popular single kind of cipher invention—and with gear arrangements, grilles, cylinders, mechanized tableaux, strip systems, and so on. (Most of these mechanisms pro-

duce substitution ciphers because of a very basic difference between substitution and transposition. A transposition cipher resembles what industrial engineers call a "batch" manufacturing process, in which quantities of material are cooked at a time, the product issuing in batches. This is because a transposition requires a whole group of letters that will all be mixed together, and it is hard for a mechanical device to store letters. A substitution cipher, on the other hand, is like a "continuous" process. Here the raw materials—letters in one case, ingredients in the other —flow continually, are not stored, and may be cut off at any point.)

Probably most ciphers get invented as a bit of recreation, as a part of the spell of interest in cryptology that so many people seem to go through. Sooner or later it occurs to every cryptologist that an acquaintance will say, "It can't be too hard to make a cipher that can't be solved." The friend then offers his theories, which often involve some crude sort of polyalphabeticity or a book code. Frequently he dredges up some system from his adolescence and, taking half an hour to put a ten-word message into that cipher, challenges the cryptologist to break it on the spot. William Jerdan, 19th-century British journalist, told in his autobiography a very typical story of the birth of a cipher, reporting with a refreshing touch of humor on the dreams of glory that often accompany the nativity.

One evening, while Jerdan and his young friends were talking, the subject of ciphers came up. Jerdan boasted that "I myself could frame a system which nobody on earth could decypher and read" and bet a dinner on it. Then somebody pulled down an encyclopedia to show him the many systems that had been invented, and, said Jerdan, "when I retired to rest fl] was on no very pleasant terms with myself, for I had looked very like what I had no chance of inventing—a Cypher." But in the morning he awoke "with a secret cypher concocted in my brain," which he discussed with his friends, among them Thomas Wilde, a future Lord Chancellor. They agreed that "It ought to be laid before the government, and I cannot tell how immense a reward I was to reap for my wonderful discovery. No castle in the air was ever more stupendous and gorgeous than mine. . . . Wilde and I were now all agog for an audience of the Prime Minister, to put him in possession of the good fortune which had befallen his government, and ourselves in the way of wealth and promotion."

[Codebreakers 405.jpg]

*Drawing of a cipher machine invented around 1888 by the French cryptologist Marquis Gaetan H. L. de Viaris. Its chief merit is that it printed its output on a strip of paper.*

They did manage to describe the cipher to a government secretary, and many years later, Jerdan, visiting a high Foreign Office official, saw a cipher being used based on his principle. He naturally thought that it was his, but it may have been invented independently by someone else.

Nearly every inventor of a cipher system has been convinced of the unsolvability of his brainchild. (The tendency to claim this in patents has, however, been receding with the rise of cryptologic sophistication.) In 1744, Leonhard Euler, the great Swiss mathematician, sent to a friend a monoalphabetic substitution cryptogram that had a few homophones, expressing his belief that it could not be deciphered. He was only slightly more naive than most inventors. A representative of the humanities, Walter W. Skeat, a distinguished English philologist and editor of Chaucer, proposed a cipher in 1896 that amounted to a Vigenere with key ABCDE; when hordes of amateur cryptanalysts knocked it off, he had the grace to bow and retire. Nearly all the cryptographic fossils entombed in dusty books or in old files of patent offices deserve their oblivion. They are too prone to error or too easy to solve or too cumbersome. Many an inventor delights in intricacy. Poorly endowed with empathy, he never considers the possibility that cipher clerks will not dote as lovingly upon the complex calculations of his cipher as he does; he fails to realize that to the clerks ciphering is not a pleasant after-hours recreation but a day-long, dull, boring job, about as exciting as adding up columns of figures, and that they would rather be out on a date with a girl friend.

Charles Babbage asserted that no man's cipher was worth looking at unless the inventor had himself solved a very difficult cipher. This rule holds true in the great majority of cases and if observed would have saved cryptologists a great deal of time. But it would be like having required Thomas Edison to pass a stiff examination in acoustical theory before deigning to look at his phonograph. The Babbage rule would have deprived cryptologists of some of the most important features of modern cryptography such as the Vernam mechanism, the rotor, the Hagelin machine. Cryptologists must process a lot of ore to get something valuable—but so must diamond miners.

In evaluating their ciphers, many inventors err by thinking that the cryptanalyst must retrace the decipher-

ment steps in his solution and that, since some of these steps are recoverable only with the key, the cipher must remain inviolate. But the cryptanalyst, of course, comes in by the back door.

Many inventors also invoke the vast number of combinations of keys afforded by their system as proof of its invulnerability. To exhaust the possible solutions would take eons, they contend. Of course the argument is specious. With 26 letters, an enormous number of different cipher alphabets is available for monoalphabetic substitution—403,291,461,126,605,635,584,000,000, to be exact. If a cryptanalyst tried one of these every second, he would need six quintillion years to run through them all. That is longer than the known universe has been in existence. Yet most monoalphabetics are solved in a matter of minutes. The reason, as mathematician Claude Shannon has shown, is that the cryptanalyst does not go after these possibilities one by one. He eliminates millions at a time. Moreover, the trials progress from the more probable to the less probable hypotheses, increasing the cryptanalyst's chance of striking the right one early. "Whereas complete trial and error requires trials to the order of the number of keys," Shannon wrote, "this subdividing trial and error requires only trials to the order of the key size in bits," a very much smaller number.

Such observations seldom have much effect upon a determined inventor. If a cryptologist points out a chink in the cryptologic armor, the inventor patches it with an extra complication. The less the inventor knows about cryp-tology, the more stubbornly will he cling to his conviction of unbreakability; and the more intelligent he is, the more ingeniously will he palter with the cryptologist. If the cryptologist objects that the cipher will not stand up to heavy traffic or will engender too many bad errors, the inventor replies that the cipher must be used properly for it to remain unbreakable. By "properly" he means the conditions that obtain only in cryptography's Utopia—no enciphering or transmission errors, no traffic volume exceeding the prescribed bounds for a particular key.

But this at once reduces his cipher to triviality as a practical method of cryptography. For with such a definition of "properly" any cipher may be regarded as unbreakable. Even a monalphabetic substitution would be used properly, in this sense, if only a single, very short cryptogram were

sent in it. The inventor, concentrating on those rare occasions on which his cipher would be used properly, refuses to see the vast domain in which it will not serve. But the ratio of the area in which a cipher will serve to the area in which it will not counts as much in evaluating it as its intrinsic merits. The cryptologist of course sees this, but when he attempts to direct the inventor's gaze to this outside world the inventor tells him, "I am not talking about that." The cryptologist and the inventor are indeed talking about two different things, and each in his way is right. The inventor is right when he says that the cipher is impregnable within its tiny duchy. But the cryptologist is even more right when he says that it is insignificant.

Classic in the annals of cryptographic invention is the case history of J. F. Byrne, who stuck with his cipher through repeated rebuffs for more than 35 years. Byrne was an intimate of James Joyce; they were students together at Dublin, and Joyce modeled Cranly in his *Portrait of the Artist as a Young Man* upon Byrne, and made Byrne's residence, 7 Eccles Street, Dublin, the home of Leopold and Mollie Bloom, the two protagonists of his great *Ulysses.** It was in 1918 that Byrne hit upon the principle

*It may not be coincidence that in *Ulysses* an inventory of Mr. Leopold Bloom's locked private drawer at 7 Eccles Street included, among other things, "3 typewritten letters, addressee, Henry Flower, c/o P.O. Westland Row, addresser, Martha Clifford, c/o P.O. Dolphin's Barn: the transliterated name and address of the addresser of the 3 letters in reversed alphabetic boustrephodontic punctuated quadrilinear cryptogram (vowels suppressed) N.IGS./WI.UU.OX/ W.OKS.MH/Y.IM: . ..." "Quadrilinear" meant to set the cipher in four lines; "reversed alphabetic" indicated the key of *a* = *z*, *b* = Y, etc.; "boustrephodontic," an adjective concocted from the adjective "boustrephodon," a technical term in paleography referring to writing that runs left and right in alternate lines, indicating that the lines of the cryptogram were to be read in that way. Unfortunately, Joyce or Bloom forgot about this in the fourth line, which incorrectly reads left to right. The cryptogram and its solution thus are:

N . I G s . m a r t h a

w d

I . U U . O X

r o f file

W . O K S . M H

dolphin s

Y . I M

barn

of his "Chaocipher," which he never disclosed publicly but was an autokey. It required nothing more than a cigar box and a few bits of string and odds and ends for its operation. When he showed it to his cousin, she exclaimed that it would bring him a Nobel Prize—not for science, apparently, but for ushering in an age of universal peace by conferring the gift of perfect security upon the communications of all nations and all men. Wrote Byrne:

> When I first set out to discover a system for concocting an indecipherable cipher, I had it clearly in mind that such a system would and should be universally available. I envisioned, for instance, the utilization of my method and machine by business men for business communications, and by brotherhoods and social and religious institutions. I believe that my method and machine would be an invaluable asset to big religious institutions, as for example the Catholic Church with its world-wide ramifications. I had, and still have in mind the universal use of my machine and method by husband, wife, or lover. My machine would be on hire, as typewriter machines now are, in hotels, steamships, and, maybe even on trains and airliners, available for anyone anywhere and at any time. And I believe, too, that the time will come— and come soon—when my system will be used in the publication of pamphlets and books written in cipher which will be unreadable except by those who are specially initiated.

Byrne corresponded with Colonel Parker Hitt, and in 1922, demonstrated his machine before Friedman and Colonel Frank Moorman, former head of G.2 A.6, then handling cryptography for the Signal Corps. They did not want it. He offered it to the State Department, which replied with a form letter stating that its "ciphers are adequate to its needs"—a statement that Byrne rightly damned as "a paragon of smugness." He submitted it to the Navy in 1937-38, negotiating apparently with Commander Joseph N. Wenger, and to A. T. & T.'s Ralzemond D. Parker, chief of company development and research and Vernam's boss when he invented the on-line mechanism. Nobody took it.

Byrne's faith remained undaunted. He had a little bro-

chure printed in which he enciphered known texts in his Chaocipher and defied the world to break it. Toward the close of his life, he wrote a book of reminiscences. It told much about his days with Joyce, but his real reason for writing it was not to shed light on early Joyce but to get his Chaocipher before a larger audience. The 21st and last chapter of *Silent Years: An Autobiography with Memoirs of James Joyce and Our Ireland,* comprising fully one eighth of the book, recapitulated the story of his Chaocipher. Byrne concluded by betting $5,000 or the total royalties of the first three months after publication of his book that no one would be able to solve the message in Chaocipher that he printed in extenso in the final pages. He flung the challenge also at the amateurs of the American Cryptogram Association and the New York Cipher Society and at Norbert Wiener, father of cybernetics, and to other believers in the capabilities of the electronic calculating machines.

Nobody ever claimed the money, and Byrne died a few years later. One may presume that the reason both for the failure of the public to read his cipher and the failure of the government to adopt it was that while the cipher probably had many merits, its many demerits outweighed them for practical use. Byrne, like many inventors, both won and lost. His cipher was never broken. But his dream never came true.

Codemaking appears to be such a popular sport because it is literally fancy-free. If cryptography is a form of abstract algebra, then inventing a new cipher system is nothing more than building abstract castles in the air with material and design of one's own choosing. To make the system work is little more than to avoid self-contradiction, yet when the answer comes out right it always satisfies the inventor. Codemaking is much more popular than codebreaking because it is easier and more esthetic; it flings together shining theories however it pleases, whereas crypt-analysis forces the mind to concentrate upon the data, upon the coarse rubble of reality. But cryptanalysis is much more rewarding. For it subdues these hard and unyielding facts; it represents a victory of the mind over something, whereas codemaking represents a triumph over nothing. This mental mastery is the keen pleasure-pang of solution; it is what men of the intellectual caliber

of Babbage and Wheatstone see in cryptanalysis, and it explains the most extraordinary testimonial ever given to cryptanalysis. The testimonial's phraseology is undistinguished and the cryptogram was elementary; what gives it its weight is that it was uttered by Harry Houdini. "I managed, after some worry, to solve the message, and very few things in after life gave me as much pleasure as did the unraveling of that code," wrote the man who, one would think, would say that about his ability to untangle the physical puzzles of knotted ropes and straitjackets and of locks on trunks thrown into the water to which he daily owed his life.

Consequently it is not surprising to learn that those addicted to this mental enjoyment have banded together to assure themselves of it. The American Cryptogram Association was founded in 1932 by members of the National Puzzlers League who wanted to concentrate more on cryptology, taking as their motto "The cryptogram is the aristocrat of puzzles." Today the A.C.A. numbers about 500 members, including some from Japan, Australia, New Zealand, India, Israel, Algeria, England, Netherlands, Spain, Northern Ireland, Germany, Sweden, Argentina, Venezuela, and Canada. Their professions are varied; included are lawyers, editors, physicians, professors, civil servants, teachers, housewives, printers, engineers, mathematicians, computer programmers, a puzzle maker, and retired people. Most of the members affect a nom de plume, or sort of sprightly codename, like B. NATURAL, AB STRUSE, FRINKUS, DR. CRYPTOGRAM; this is a carry-over from the National Puzzlers League and is alleged to increase informality among the membership. Every other month, the association publishes *The Cryptogram,* a magazine usually of 24 pages with articles on cryptanalysis, new ciphers, and cryptologic history. It offers the members several kinds of cryptograms for solution—monoalphabetics with word divisions ranging from the simplest to the kind with the most twisted syntax and vocabulary (these are called "Aristocrats" in recognition of the association's motto), monoalphabetics without word divisions ("Patristocrats"), cryptograms in all the varieties of cipher that can be solved within the compass of a 150-letter message, sometimes with tips, and cryptograms in foreign languages, including occasionally Esperanto, Latin, and Hungarian. Solvers' noms and scores are listed. The association holds

an annual convention at which members hear talks on cryptology, engage in a cipher contest, are interviewed by slightly befuddled newspapermen, and banquet. In the larger cities, members have banded together to form local groups, such as the New York Cipher Society, which usually meet monthly to talk, exchange ideas, and socialize. The association appears to be the only one of its kind in the world.

While many people make and break ciphers in sport, others do it in earnest. The variety and quantity of non-political cryptography can only equal the number of motives that impel people to secrecy, and these motives, like their ciphers, are most heterogeneous.

In the graveyard of New York's Trinity Church, on Broadway at the foot of Wall Street in the very heart of the financial district, stands a tombstone with an epitaph partly in cipher. Under it lies James Leeson, who died September 28, 1794, aged 38. The cipher inscription is in the ancient pigpen cipher, whose use goes back hundreds of years, and it reads *Remember Death.* Why Leeson had it carved there no one, perhaps, will ever know, but his motive may well have been that of the ancient Egyptians who first used cryptography in their sepulchral inscriptions: to stay passersby and bring the dead to life in their memory.

More obscure are the motives that led several people to encipher entries in church registers, though the conjectures can be tantalizing. At Cleator, Cumberland, England, someone used the very simple cipher

ae ioulmnr 123456789

with the rest of the plaintext letters left unenciphered to record in Latin the baptism on January 1, 1645, of Janet Barne, daughter of William Barne, curate of the parish. The mother's name is not given. Could the encipherer have been Barne himself? And if so, was he perhaps hiding an illegitimate birth? The same system was used in the fee-book for the parish of Iver near Uxbridge, England, to note on January 17, 1767, the marriage of 188 b58y48. Why Ann Bunyon's name should be veiled while her husband's was left in clear remains unknown.

In two spirals on a minute of a letter of September 14, 1750, Gabriel Cramer, a teacher of mathematics at the I Calvin Academy in Geneva, who corresponded with the most learned men of his time, inscribed two cipher messages. Simple columnar transpositions, they counseled: "The oracle tells thee to fear nothing; thou art permitted to hope for everything; dare boldly; banish fear; thou canst surely give thyself over to joy." Cramer almost certainly •composed the messages only for his own pleasure or en-Icouragement, perhaps choosing the spiral because it sym-Jbolized unrolling time and so a future to which he may have looked forward.

Cryptography has protected not only personal secrets, but spiritual ones as well. Secret societies have long used ciphers. The Free and Accepted Masons monopolized the antique pigpen cipher to such an extent that it is often called the Freemasons' cipher. Its most common modern form is this:

[Codebreakers 413.jpg]

Thus *Scottish rite* would be enciphered These symbols stand out here and there in the printed manuals of Masonry; they comprise part of the mixture of cryptography, abbreviation, and rebus with which the Masons diguise their secret rituals. In the postbellum South, the Knights of the Golden Circle, a kind of Ku Klux Klan, used essentially the same cipher for their occasional cor-

| respondences.

More recently, Alfred C. Kinsey and his associates

| encoded the replies of interviewees about their sexual habits for *Sexual Behavior in the Human Female.* Only four persons on the staff of the Institute for Sex Research could read the code, which recorded the answers in the forms of x's and a few checks, dashes, and incomprehensible abbreviations in columns. Kinsey explained that "Recording the data in code in the presence of the subject has done a good deal to convince him or her of the confidence of the record. Even though anonymity is ordinarily guaranteed by the statement which caps most questionaires, many persons still fear that there may be some means by which they can be identified if they write out answers to printed questions. They fear, and not without some justification in the history of such studies, that a record made in plain English may be read by other persons who obtain access to the file. It is not to be forgotten that our sex laws and public opinion are so far out of accord with common and everyday patterns of social behavior that many persons

might become involved in social or legal difficulties if their sexual histories became publicly known."

Lovers could sometimes find themselves in the same difficulties if their liaisons became known. Consequently Ovid, in his *Art of Love,* offered counsel on how to correspond clandestinely, mentioning some primitive forms of secret ink:

> Tuta quoque est fallitque oculus e lacte recenti
> Littera:  carbonis pulvere tange, leges.
> Pallet et umiduli quae fiet acumine lini,
> Et feret occultas pura tabella notas.

Or: "A letter is also safe and escapes the eye when written in new milk; touch it with coal dust and you will read. That too will deceive which is written with a stalk of moistened flax, and a pure sheet will bear hidden marks." He also advised using pronouns of the opposite sex, such as HIM for *her.*

Among the strange means of secret communication to which lovers in the 1800s resorted was perhaps the most public of all channels—the personal advertisements in newspapers, sometimes called the "agony columns." Apparently unable to contact one another directly through the mails because of parental or other restrictions, the lovers could easily bring a newspaper into the house and thus receive their messages. For secrecy, these were enciphered, but usually in so elementary a system that anyone who applied himself could read their intimacies. In February of 1853, *The Times* of London carried a Caesar substitution, in which *a=v,* addressed to Cenerentola: *Until my heart is sick have I tried to frame an explanation for you, but cannot. Silence is safest, if the true cause is*

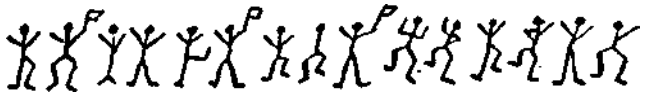
*not suspected. If it is, all stories will be sifted to the bottom. Do you remember our cousin's first proposition? Think of it.* A few months later, on August 19, the same paper carried a cryptogram in an ordinary reversed alphabet— a = z, *z* = A—with numbers representing a few words like *the* and *that.* The message began *My darling, need I say how delighted I was to receive your letter of dear remembrance on my birthday? I beg you not to think 1 wrote under any irritation. I fear my letters being read by others.* . . . Wheatstone and fellow scientist Charles Babbage often solved these simple missives. Babbage easily read a Caesar substitution of May 13, 1859, addressed to Robert: *Why do you not come or write for me? Such grief and anxiety!—Oh! Love Love!* His most difficult was a numerical cryptogram of December 21, 1853, addressed to Flo and beginning 1821 82734 29 30 84541. After, apparently, months of trying it as a polyalphabetic and as a homophonic substitution, he finally discovered that it was a polyphonic substitution, in which each cipher number stood for from one to four plaintext letters. It began (with two enciphering errors): *Thou image of my heart!*

Sometimes people inserted cryptograms just to see if anyone would make them out. A piece of advice about education, enciphered in a Caesar substitution, dated Kensington, was followed a week later by a cleartext advertisement addressed to Kensington, saying, *Your cipher is made out; but such good maxims should be written in plain English, that all might benefit.* On February 10, 1852, *The Times* was used to circulate calumny against itself—in cryptographic form, of course: TIG TJOHW IT TIG JFHIIWOLA OG TIG PSGVW. It stood for *The Times is the Jefferies of the press,* enciphered in a progressive Vigenere with key ABCD . . . beginning anew with each word. The reference to George Jeffreys, a 17th-century English judge, meant that *The Times* was a pusillanimous tool of the government and mercilessly severe to its opponents. When the editor of *The Times* heard about the cryptogram, he, like his queen, was not amused. The family of the explorer Richard Collinson communicated with him privately during his explorations even though they did not know where he was by inserting coded personal notices in *The Times.* Use of the enciphered personal advertisement seems to have died out, however, perhaps owing to the censor-

ship restrictions of two world wars, perhaps because of the telephone or relaxed parental restrictions.

Cryptology has enriched literature in other ways. Many of the authors of antiquity—among them Homer and Herodotus—mention secret writing. But they allude to events believed to be historical. Not until the Renaissance, when cryptology became more widely used and hence known to many literate men, could it serve as a topic in literature. *The* first author to employ it was Rabelais, who in an exuberant section of *Pantagruel* satirizes the whole business of unearthing secret writings. Shakespeare mentions interception, if not cryptanalysis, in *Henry V,* but it was Edgar Allan Poe in "The Gold-Bug" who first used cryptology as a central element. The tale not only offers one of the clearest expositions of the solution of a secret message, but the result of that solution—the discovery of a hidden treasure—renewed mystical vibrations between cryptology and magic, and reglamorized cryptology. Jules Verne, too, heightened the suspense of several of his futuristic novels with the mystery of secret writing.

But the greatest feat of fictional cryptanalysis was performed, naturally enough, by the greatest of fictional detectives. Sherlock Holmes's thorough knowledge of the subject becomes manifest in his "Adventure of the Dancing Men." The dancing men—little stick figures with their arms and legs in various positions—constitute the cipher symbols. An American gangster, Abe Slaney, "the most dangerous crook in Chicago," writes threatening notes in them to a former childhood sweetheart, Elsie, who has married an English squire. The squire copies the messages, which are chalked on window sills and tool houses, and brings them to Holmes. Holmes solves them, but the squire is killed by Slaney in an exchange of shots before Holmes can prevent the tragedy. Slaney escapes. Holmes, who



*A message in the Dancing Men cipher, solved by Sherlock Holmes*

knows where he is from the solved cryptograms, carefully composes a message out of cipher symbols that he has recovered and sends him a note urging him to *Come here at once.* (Holmes perhaps borrowed this scheme from Thomas Phelippes, who, Holmes knew, had in 1587 forged a cipher postscript to a letter of Mary, Queen of Scots, to learn the names of the intended murderers in the Babing-ton plot against Elizabeth.) Slaney, naively believing that only Elsie and others of his Chicago gang at the Joint ould read the cipher and that the note must therefore .ve come from her, returns to the squire's home. He is .t once arrested and,

naturally, confesses.

Holmes is, as he himself says, "fairly familiar with all forms of secret writings, and am myself the author of a trifling monograph upon the subject, in which I analyse one hundred and sixty separate ciphers, but I confess that this is entirely new to me." He referred, of course, to the use of the dancers "to give the idea that they are the mere i random sketches of children," and not to their nature as a *I* monoalphabetic substitution. That he promptly recognized that they belonged to this class of ciphers is proved by his embarking at once upon a solution without any false starts. His task was considerably more difficult than that of any other fictional cryptanalyst, because bis text was exceedingly short, disconnected, and elliptical and loaded with proper names. It eventually consisted of five messages in telegraphic English: (1) *Am here Abe Slaney,* (2) *At Elriges,* (3) *Come Elsie,* (4) *Never,* (5) *Elsie prepare to meet thy God.* But to begin with Holmes had only the first message, on which he made his start, and he broke the cipher only with that message plus the next three. They total only 38 letters, eight of them occurring but once; out of the nine words, four are proper names, and of the other five none is among the ten most frequent words in English, which normally make up a quarter of English text.

The difficulty of such a solution demonstrates the power and flexibility of the great detective's mind. Holmes would quite evidently have preferred to solve the cryptogram with his usual rigorous deductions, which means by frequency analysis. He began that way. The first message contained 15 dancing men, of which four are in an ecstatic spread-eagle position and three have their left leg bent. Holmes at once marked down the four spread-eagle dancers as *e.*

in I Now, neither letter frequencies nor any other statistical

phenomena are reliable in small samples; it was quite possible that the three bent-left-leg dancers represented *e,* or that one of the single dancers did, or even that no *e* at all occurred in the first message. It is inconceivable that Holmes did not know this. Nevertheless, he fixed the symbol for *e* "with some confidence." He was right, of course, but why? No doubt Holmes, having recognized that the figures holding flags marked the ends of words, noticed that two of the four spread-eagle dancers carried flags, and instantly connected this with the well-known fact that *e* is the most frequent terminal letter in English. His swift mind may also have observed the variety of the *e* dancers' contacts. But all this flashed through his great brain just below the threshold of his consciousness—this perhaps helps explain the characteristic rapidity of his deductions—and consequently he did not articulate it in his explanation to Watson. Or perhaps he did not want to burden Watson with all those details.

He did realize, however, that neither frequency analysis nor anything else could go further in the first message, and so he awaited more text. Upon the arrival of the next three messages, he saw that frequency analysis would not serve with so short a text. Unable to progress with his beloved deductions, he deftly switched to induction. He performed brilliantly, guessing first that a five-letter word with *e* as the second and fourth letters and comprising a message in itself must be *never,* and then conjecturing that the name *Elsie* might occur in the messages and finding it. With these values he was fairly on his way, and with further arduous labor completed the solution.

Some cryptologists have affected to sneer at Holmes's taking two hours to solve these cryptograms, covering "sheet after sheet of paper with figures and letters" as he did so. With so short and difficult a text, however, the time is not only understandable, but admirable/ Moreover, the dancers caper in no recognizable pattern when placed in alphabetical order, and when they pose in a graduated order of choreography, no regularity appears in the letters. In other words, the cipher of the dancing man is purely arbitrary. Some members of the Sherlock Holmes fan club, the Baker Street Irregulars, which included Alexander Woollcott, Christopher Morley, and Franklin D. Roosevelt, have kept their gaslights burning late in attempts to dis-

cover a regular basis of construction. It is wasted energy. The fact that Holmes limited himself to already recovered letters in his "Come here at once" message to Slaney suggests that he did not discover any regularity which would have permitted him slightly more latitude in composing that message. And surely had there been such a key pattern, Holmes would have discovered it. The inventor of the cipher, Elsie's father, Patrick, "the boss of the Joint," may have gotten the idea for the dancing men from a cipher based on human figures in the semiofficial *Manual of Signals* by Albert Myers, the founder of the "U.S. Army Signal Corps, or from the same unknown place as the inventor of a slightly later United States patent that uses manikins for cipher symbols, or from the ubiquitous Carbonari, whose call-sign is made by extending the arms horizontally in the form of a cross and the reply by pressing two fists one above the other on the breast. Holmes may well have known of these possible sources. But even if Patrick did borrow the idea from one of them, he has altered the arrangement so thoroughly that cryptanalysis is left as the only way of resolving the problem.

A final point remains to be cleared up in the case of the dancing men: the source of the cryptographic errors that appear in all printed accounts. In the very first publication of "The Adventure of the Dancing Men," the cryptograms use the same dancer for the *v* in *Never* and the *p's* in *prepare,* and use an identical dancer for the *b* in *Abe* and for the *r* in *Never.* The Baker Street Irregulars have expended a great deal of energy on this problem. It is in their attempts to find the "correct" version that they have falsely assumed a regularity in the cipher alphabet, constructing tables of arm and leg positions and extrapolating the ciphertext symbols for the eight letters (/, /, *k, q, u, w, x, z,)* that do not occur in the messages. They have also sought to determine the cause of the errors. Their efforts, however, have served only to show why they are the disciples and Holmes the master. All of them engage in armchair thinking without investigating the facts. There has been a suggestion that the errors "are in the messages of the villain of the story and may be laid, if one so wishes, to the poor devil's confusion and despair," but no one has raised the equally likely possibility that the squire may have made the mistakes while copying the messages

to bring them to Holmes. In fact, however, the errors are neither Slaney's nor the squire's, for the errors were not present when Holmes solved the cryptograms. If the same symbol had been used for *v* and *p* in the originals, Holmes would have produced the partial plaintext *vrevare* in the fifth message after guessing *Never* instead of the *?re ?are* that he shows, with the two *p's* as unknowns. Similarly, if the *r* and *b* had been confounded in the original, he would have shown a partial solution *?re* (for the correct *Abe)* after guessing *Never,* but in fact he shows a partial solution *??e* with the *b* still unknown. Holmes' own account thus proves that the errors did not exist in the original messages—and it is fortunate that they did not, for they occur at junctures crucial to the analysis and, coupled with the other difficulties, might have rendered the cryptograms almost impossible to read, even for Holmes. The errors must therefore have been made by Dr. Watson in transmitting the canon to the world. Later publications have compounded Watson's original errors, but these have passed through the hands of literary and journalistic types, notoriously frivolous and unreliable as to facts, and need not be considered.

Just as real-life criminals seem to be less exciting than their fictional counterparts, so cryptology seems to have been used far less in life than in the pages of detective fiction. Indeed, the only major use of codes and ciphers by criminals came during the American Prohibition era in the 1920s and early 1930s. The bootleggers' attempts to smuggle liquor past American law-enforcement agencies required coordinating the movements of ocean-going vessels with the small speedboats that would bring the cases of bottles ashore. For this they used radio, and they coded their messages. But many succumbed to the brilliant analyses of Mrs. Elizebeth S. Friedman, wife of William F. Friedman, who served as a cryptanalyst for the Coast Guard, helping it to keep out the smugglers.

As a result of the information obtained from crypt-analysis and from direction-finding, the Coast Guard put increasing pressure on the smugglers' activities. Evidently the bootleggers discovered the weakness of their wireless operation, particularly their codes and ciphers, for in two years their radio and cryptographic organizations ramified at an enormous rate. Whereas in 1927-28 only two general systems were in use, changed only every six

months, in mid-1930 practically every rum boat on the Pacific Coast had its own code or cipher. In May of 1930, for example, the Consolidated Exporters Corporation, with three shore stations, employed a different crypto-system from its headquarters to each of its "blacks," or rumrunning craft, while the mother ship corresponded with these blacks in an entirely different system. In the fall of 1929, this giant, which had gobbled up most of its competition in the Pacific, established a branch in Belize, British Honduras. Traffic in this Gulf Coast branch rapidly climbed to several hundred cryptograms a month. On the Atlantic side of Florida, 25 cryptograms a day were intercepted, while in the New York region, in only five days in February of 1930, a radio inspector heard no fewer than 45 unlicensed stations from within ten miles of New York. They were involved in operations from Nova Scotia to the Bahamas. It was reported that one syndicate paid its radio expert $10,000 a year—this during the Depression! A retired lieutenant commander of the Royal Navy devised the systems for Consolidated Exporters' Pacific operation, though its Gulf and Atlantic groups made up their own as needed.

His name was unknown, but his cryptologic expertise was apparent. The smugglers' systems grew increasingly more complicated. "Some of these are of a complexity never even attempted by any government for its most secret communications," wrote Mrs. Friedman in a report in mid-1930. "At no time during the World War, when secret methods of communication reached their highest development, were there used such involved ramifications as are to be found in some of the correspondence of West Coast rum running vessels." One such system, employing two different commercial codes, passed through five steps: The clerk (1) encoded the plaintext in the commercial *ABC Code,* 6th edition, (2) added 1000 to the numerical codegroup, (3) looked up this codenumber in another commercial code, the *Acme,* (4) transcribed the codeword opposite that codenumber, and (5) enciphered that codeword in a monoalphabetic substitution. Much of this complexity, however, was vitiated by the clerk's habit of only partially encoding messages and enciphering the rest in a monoalphabetic substitution that appears to have been the same as for the code. Mrs. Friedman illustrated

the process with an actual message (which may have some slight errors in it):

| | |
|---|---|
| *plaintext* | Anchored in harbor. Where and when are you sending fuel? |
| *in* ABC Code | 07033 52725 24536 |
| +1000 | 08033 53725 25536 |
| Acme Code *word* | BASHY ouvs WINUM |
| *substitution* | MJFAK ZYWKH QATYT JSL QATS QSYGX OGTB |

In her office—first in a building near the Bureau of Printing and Engraving, then in a building on Pennsylvania Avenue opposite the Willard Hotel—Mrs. Friedman solved 12,000 messages in just her first three years for the Coast Guard, the Bureau of Customs, the Bureau of Narcotics, the Bureau of Prohibition, the Bureau of Internal Revenue, and the Department of Justice. Her testimony in court as to her solution of various messages sent criminals to jail more than once. The ringleaders of Consolidated Exporters were convicted and sentenced after she testified to the secret meaning of its intercepted cryptograms. "Without their translations," the prosecutor later wrote to Mrs. Friedman's chief, "I do not believe that this very important case could have been won."

Most businessmen, like most criminals, hardly ever use cryptography for communications. An occasional price code is about as far as they go. Many inventors, contemplating the principle that the competition of free enterprise entails secrecy, have thought that they would grow rich by selling cipher machines to businessmen. None have succeeded, and many have failed. The successful Hagelin firm sells less than one per cent of its output to private firms. Banks and companies in highly competitive fields such as mining and oil sometimes use cipher machines. But for the vast majority of businesses, the difficulty for a rival firm of obtaining copies of telegrams means that no special precautions are necessary. And business espionage seems rarely to have gone as far as cryptanalysis.

The one known case stands out. A firm in Hong Kong obtained the messages of a rival firm from an employee of a cable office. These had been encoded with a commercial code that was sold publicly, and the intercepting firm had no trouble reading the messages—and then submitting bids of its own that were half a cent lower than

those of its rival, thus stealing considerable business. When the other firm learned about this, it began enciphering its code messages. Evidently this proved too much for the intercepting firm, for it no longer won bid after bid.

In only one field has commercial cryptography had even a moderate success: telephone scramblers. The increased fear of wiretapping has led increasing numbers of business executives to purchase scrambler attachments for their telephones. Prospecting teams will carry a scrambler with them so they can report the location of mineral deposits without fear of being overheard. But not all businessmen use scramblers to protect commercial secrets. A substantial percentage give the other half of the scrambler set to their mistresses!

## 19. Ciphers in the Past Tense

ALL CRYPTANALYSTS have not borne arms for Mars. Some of the most prolific have served Cilo, the muse of history. Many of these unsung heroes—the only cryptologists whose contributions enlightened all mankind—worked in the 19th century. The immense influence of Leopold von Ranke's objective school of history, which demanded a study of the original documents, sent droves of historians to mine state papers and diplomatic correspondence in the archives, whose doors had been unlocked for the first time by the nationalism and democracy of the 1800s.

The researchers found many of the documents in cipher, or partly so. Invariably, it seemed, the crux of a dispatch was enciphered. In the mid-1500s, a Venetian ambassador wrote home about his talk with Henry II of France concerning English affairs. "His Majesty suddenly turned to me, taking a troubled aspect and shrugging his shoulders, added to me these very words. . . ." and the rest is in cipher! Historians realized that the most important parts were the most likely to be put into cipher. Some, unfamiliar with cryptanalysis, apparently regarded the resultant cryptogram as an act of God, an insuperable obstacle which they would have to live with as with a hole in the document. "Were we able to decipher the letters

written on congressional politics by Richard Henry Lee and his correspondents ... no doubt much of the cloud which hangs over the congressional intrigues of that critical period would be removed," mourned Francis Wharton in 1889 in *The Revolutionary Diplomatic Correspondence of the United States.*

But other scholars looked upon the cryptograms as a challenge. One of the first of these was a transplanted German whose services to English historiography were of high importance.

Gustave Adolph Bergenroth was born February 26, 1813, at Marggrabowa, which his biographer called "an insignificant town in the remotest and dreariest corner of East Prussia." He attended the University of Konigsberg, where he was very popular with his fellow students and where he sustained a severe injury to his right wrist in duelling. After working in Cologne and Berlin as an assessor, with time out for a trip to Italy necessitated by his liberal views, he quit his job and sailed in 1850 for California as a pioneer. The racy style of his first composition in English, "The First Vigilance Committee," drew favorable attention, and he determined to write. After some literary work, he began a history of Tudor England. Finding the available materials insufficient, he set out, late in his forties, for that great repository of documents for those years when Spain bestrode the world, the Archivio General at Simancas in northwest Spain. His letters home soon won him a stipend from England's Master of the Rolls to find, list, and summarize the state papers at Simancas that related to English history and to prepare a volume for the Spanish series of the endless Calendars of State Papers. He forgot his Tudor history.

He arrived at Simancas in September, 1860, and established himself in a kind of hotel, the Parador della Luna, where he would do much of his cryptanalysis. An Englishman who visited him painted the scene: "Simancas is a collection of wretched hovels, half buried in dust and sand. There is not a good house in the place. The one in which Mr. Bergenroth lives belongs to a farm bailiff, consists of two storeys, all the rooms of plaster, and the floors of brick. No fireplace in any of the rooms, and, as the winter is very intense here from November to February, and the walls full of holes, nothing but the strongest desire to do service to history could reconcile

any man to so much hardship." Bergenroth had, moreover, to overcome some of the oddest phenomena ever to interfere with cryptanalysis. The plaza beneath his room was crowded with shouting donkey-drivers and visited frequently by a dulciana, whose "shrill notes, continually playing an air from Traviata and one Spanish melody, and nothing else, drive me almost mad." His landlady liked to strum on her guitar, and "none but drivers of bullock-carts could, for a single night, stand the music of the Lady della Luna." The kitchen girl "hangs my linen and that of the whole family over my balcony for drying, and then, with laudable resolution, sets to ironing it on my writing-table."

More troubles faced him at the Archivio General. It consists of an old castle, with crenellated walls pierced by loopholes, surrounded by deep moats and drawbridges. Its 46 rooms contain more than 100,000 bundles, or legajos, in each of which are filed from 10 to 100 documents, making a total of several million. From this staggering accumulation Bergenroth had to select the pertinent items. It was hard for him even to get at them. When Spain's archives administration finally granted him entree, the crabbed Renaissance semiuncials made long and dogged practice necessary before he could read the handwriting. Indeed, the archivist himself had often been defeated by it, and in his jealousy at Bergenroth's success he deliberately hampered the historian's work by refusing access to such cipher keys as were in his possession. Bergenroth had to recover them by himself, as well as those keys^ that had been lost.

The story of his cryptanalytic endeavors can be pieced together from several of his writings.

> I did not go to Spain quite unprepared for my work. I had carefully studied the *Paleographie* of Christoval Rodriguez; I have also spent much time in deciphering such old Spanish documents as were to be found in the libraries of London and Paris. . . .
>
> [At Simancas.] The first thing I considered it necessary to do was to study most carefully, not only the Spanish orthography of the period, but that of each statesman in particular who could be supposed to have written any of these letters. Even this was not sufficient. I had to study the turns of thought,

and the favourite words and expressions of each statesman. Long and curious lists, covering many sheets of paper, lay during many months on my writing-table, and were stuck up against the wall of my room.

I did not discover any of the keys to the ciphers in a methodical manner. Whilst engaged in copying I was constantly on the watch for a weak point, convinced that no man can for any length of time succeed so completely disguising his thoughts but that he will occasionally betray himself to a close observer. Wherever I thought that that was the case, I tried to guess the meaning of the signs. A hundred times I may have done so in vain, but at last I triumphed.. . .

When copying an instruction to the Duke [de Estrada], I discovered little dots, like full stops, behind two signs of cipher. As interpunction is never used in cipher of this kind, the dots could only be signs of abbreviation. But even abbreviations (a skilful writer would never have made use of them) offer so many difficulties that they can be employed only on the most common occasions, as, for instance, V. A. for Vuestra Alteza, or n.f. for nuestra fija, or nuestro fijo. From obvious reasons [in this case], I decided in favor of "nuestra fija," and inferred further that the preceding signs must correspond to "princesa de Gales." The breach was opened, and before three o'clock in the next morning I was in possession of eighty-three signs, representing the letters of the alphabet, and of thirty-three monosyllables, signifying words. The key is far from being complete, but there remain no longer unconquerable difficulties .... [This cipher] of the Duke de Estrada is the most difficult, and at the same time the most important of all, as a greater number of undeciphered despatches are written in it than in any other kind of cipher. . . .

The question may be asked, whether my decipherings are trustworthy? I answer with full confidence in the affirmative. I have more reason than one for doing so. After I had deciphered the despatches, I found, in some instances, that they were only ciphered copies of drafts in plain writing. Thus I had an opportunity of comparing my interpretations with the originals, and found that in all essential points

> they were identical. The key of De Puebla and the fragments of the two other keys, which were given to me after my return form Madrid, provided me with an additional test. The keys which I had already formed before seeing them coincided perfectly with them. . . . But the general and most decisive proof consists in the meaning of the despatches, concealed behind the cipher.

In ten months, Bergenroth surpassed the feats of many professional cryptanalysts by reconstructing 19 nomencla-tors—an average of about one every two weeks, some with 2,000 or 3,000 elements. This was in addition to his own copying, his supervising of a copyist, his searching for documents, his battles with the bureaucracy, and his frequent letters home. He did not like the cryptanalysis: "Nothing but sheer necessity would have forced me to attempt such a task, which, I think, is one of the most laborious that any man could undertake." Yet by July 23, 1861, ten months after his arrival, he could report, "The despatches in cipher are all copied and deciphered, with the exception of two small letters (the one of them from John Stile to Henry VII), which I intend to decipher in Barcelona or in London. I am now too fatigued for a work which requires so much concentration of thought as the discovery of keys to unknown cipher does." He did solve the Stile letter, but not the other, a short one from King Ferdinand and Queen Isabella dated at Segovia on August 20, 1503, the only one in that key. This key was the only one of those used by Spain during the reign of England's Henry VII (1485-1509) that he failed to read.

One long dispatch, whose solution took a week, typifies the treasures he unearthed. It is a letter of July 25, 1498, from Don Pedro de Ayala in London to Ferdinand and Isabella, reporting on England's fitting out of an expedition to some islands in the New World which, Ayala thinks, had already been discovered by Columbus and were owned by Spain. He apparently referred to the second voyage of John Cabot, on whose discoveries the English claims to North America rested. Though some of the nomenclators that Bergenroth recovered were later found in the archives, many others never were, and only his cryptanalyses brought the documents to light. Bergenroth died *in* 1869 of a fever contracted at Simancas, but the results of his labors shine today in the close-printed pages of his *Calendars of Letters, Despatches, and State Papers Relating to the Negotiations Between England and Spain.*

[Codebreakers 428.jpg]

*Gustave* Bergenroth's reconstruction of a Spanish cipher.

To their resumes of hundreds of documents, the historians return time and again, with gratitude.

The longest, the best known, the most tantalizing, the most heavily attacked, the most resistant, and the most expensive of historical cryptograms remains unsolved. It fills an anonymous, untitled volume that has been called "the most mysterious manuscript in the world." In *1962,* rare book dealer Hans P. Kraus of New York attracted worldwide attention when he asked $160,000 for this book that no one can read.

1

The volume itself is unprepossessing. A large octavo of about 6x9 inches, it has 204 pages; 28 others are lost. Its covers, of vellum like the leaves, are off. Dozens of tiny female nudes, astrological diagrams, and about 400 drawings of fanciful plants illuminate the book in blue, dark red, light yellow, brown, and an especially vivid green. Running among these decorations is the text itself. The manuscript somewhat resembles an herbal—a book, common in the Middle Ages, listing plants with medicinal properties and often giving recipes for extracting drugs from them.

At first glance, the text that is the heart of the mystery appears to be no problem at all. It does not look cryptic. It looks like ordinary late-medieval handwriting. The symbols preserve the general form of letters of that time, which they are not; they are like old friends whose names are on the tip of one's tongue. The writing flows smoothly, as if a scribe were copying an intelligible text; the symbols do not seem to have been printed one by one. In the most cursory examination of a single page, the eye recognizes the same letters again and again, and then it sees repeated groups and even repeated words, sometimes with slightly different endings.

All this sounds as if the text, if not in a known language disguised to the modern eye by the unfamiliar handwriting, should be in some easily ascertainable tongue. Yet scholars in the most recondite languages have stated that they could not understand it. Palaeographers have declared that the script was not known to them. And cryptanalysts, whose frequency counts of the approximately 29 symbols (some blend into others and are hard to define) looked like those of an ordinary monoalphabetic substitution, and who laughed to themselves when they spotted all those repetitions that this would be simpler than the puzzle cryptograms in newspapers, turned away in chagrin when their attempt to resolve the text into church Latin, or Middle English, or langue d'oc, or some other appropriate tongue, failed utterly.

This is not to say that no one has ever claimed to have solved it. Indeed, one solution that was announced temporarily transformed the manuscript into perhaps the most important document in the history of science. Unfortunately, it, as well as the others, has been disproved.

Mystery has beclouded the manuscript since its recorded

history began. That was on August 19, 1666, when Joannes Marcus Marci, the highly respected rector of the University of Prague, sent the book to his former teacher, Athanasius Kircher, the most famous Jesuit scholar of his time. Kircher had, three years earlier, published a book on cryptology and a universal language, and had boasted of having solved the riddle of hieroglyphics. In a letter accompanying the book, Marci recalled that the former owner of the book had sent Kircher a portion of the text for possible solution. To that work the owner "devoted unflagging toil . . . and he relinquished hope only with his life. But his toil was in vain, for such Sphinxes as these obey no one but their master, Kircher. Accept now this token, such as it is and long overdue though it be, of my affection for you, and burst through its bars, if any there be, with your wonted success." Bars there were, but Kircher, who never shrank from bragging of what he thought were his successes, did not burst through them, for his silence on this point is eloquent.

Marci wrote that the manuscript had been bought for 600 ducats by the Holy Roman Emperor Rudolf II. More of a scholar than a ruler, Rudolf founded observatories for Tycho Brahe and Johannes Kepler, established a botanical garden, and set up an alchemical laboratory to which he invited numberless scientists. The presence of the manuscript at his court in Prague was later proved by the discovery in a margin of the autograph of Johannes de Tepenecz, a Bohemian scientist who was a favorite of Rudolf.

Marci also reported the belief that the author of the manuscript was Roger Bacon, the English Franciscan friar who lived from about 1214 to 1294. Bacon had speculated, centuries before they became reality, on the possibility of microscopes and telescopes, motorboats, horseless carriages, and flying machines. Popular legend credited him with great magical abilities, a reputation probably enhanced by his extensive writing on alchemy. He interests modern science because of his precocious emphasis on observation of natural phenomena, so unlike the a priori scholasticism of his time. He is not to be confused with Sir Francis Bacon, the English statesman who lived from 1561 to 1626, wrote the famous *Essays,* and largely shaped modern science through the influence of his philosophy—although that philosophy, insisting upon induction and experimentation, does bear a strange kinship to that of his medieval namesake.

[Codebreakers 431.jpg]

*A page of the Voynich manuscript*

Presumably Roger Bacon would have written the manuscript in cipher to

conceal secrets that, if publicized, would have left him open to the grave medieval charge of black magic.

But how did a manuscript attributed to Roger Bacon get to Rudolf's court at Prague? Between 1584 and 1588, one of the Emperor's most welcome visitors was Dr. John

Dee, an English divine, mathematician, and astrologer who is sometimes said to have been the model for Prospero in *The Tempest.* Dee shared Rudolf's interest in the occult and was an enthusiast for Roger Bacon, manuscripts of many of whose works he had collected. He knew the young Francis Bacon and may have even introduced him to the works of Roger Bacon, which may help explain the similarities in their thought. Dee may have been aware of Roger Bacon's own brief discussion of cryptography in the *Epistle on the Secret Works of Art and the Nullity of Magic.* He certainly had some knowledge of, and considerable interest in, cryptology, for in 1562, he bought for Sir William Cecil, Queen Elizabeth's great minister, a manuscript of Trithemius' "Steganographia," which had not yet been published and "for w°h a Thowsand Crownes have ben by others offred, and yet could not be obteyned," Dee spent ten days "with contynuall Labor and watch" in making himself a copy.

It may be that Dee had somehow obtained the mysterious manuscript (possibly from the Duke of Northumberland, who pillaged many religious houses when Henry VIII broke up the monasteries, and with whose family Dee was associated), was told or assumed that it was Bacon's, tried to solve it, and, failing, made a gift of it to Rudolf, perhaps on behalf of Elizabeth, for whom he was serving at Rudolf's court as a secret political agent. The English physician and writer Sir Thomas Browne (who, incidentally, first used the word "cryptography" in English) related that Dee's son, "Dr. Arthur Dee (speaking about his father's life in Prague) told about . . . book containing nothing but hieroglyphicks, which book his father bestowed much time upon, but I could not hear that he could make it out." The comment may refer to this very manuscript.

This is conjectural, however. What is certain is that Kircher deposited the manuscript in the Jesuit Collegium Romanum, and that in 1912 an American rare book dealer named Wilfred Voynich purchased it for an undisclosed sum from the Jesuit school of Mondragone in Frascati, Italy.

Eager to read the manuscript, Voynich generously supplied photostats to anyone who seemed likely to solve it. Many tried. Botanists thought they could read it-by identifying the plants and assuming their names as probable words; one difficulty here was that most of the flora were

imaginary. Astronomers recognized stars such as Aldebaran and the Hyades but could not force a solution. Philologists tried the methods used for reading lost languages and failed. Cryptanalysts observed characteristics in common with ordinary ciphers and found that it resisted their well-tried techniques. Voynich heard from many specialists who were interested in the problem: palaeographer H. Omont of Paris' Bibliotheque Nationale, who had written a learned article about a 15th-century cryptographic manuscript on alchemy; Professor A. G. Little, a foremost authority on Bacon; a Harvard professor of anatomy; George Fabyan of the Riverbank Laboratories; the vice president of the Royal Astronomical Society in London; even Dom Aidan, Cardinal Gasquet, prefect of the Vatican Archives, who offered to help get any documents from those archives that might throw light on the problem. Almost certainly many of these and others tried to solve the cryptogram. Among the others in 1917 was Captain John M. Manly, then second in command of Yardley's MI-8. He had cracked the Lother Witke cipher that had baffled all his colleagues but, like the others, with the Voynich manuscript he failed. And so did Yardley.

In 1919, some of Voynich's reproductions found their way to William Romaine Newbold, a professor of philosophy and former dean of the Graduate School at the University of Pennsylvania. Newbold, *54,* a brilliant man who had stood first in his class of 1887 at Pennsylvania, had wide-ranging interests, many of which had in common an element of the occult—spiritism, the Gnostics, the Great Chalice of Antioch, supposed by some to be the actual chalice of the Last Supper, which, is known in legend as the Holy Grail. He knew many languages and later became proficient in cryptanalysis: in 1922, Theodore Roosevelt, Jr., then Assistant Secretary of the Navy, thanked him for his "time and trouble in deciphering espionage correspondence that had baffled the Department here in Washington."

Newbold saw microscopic shorthand symbols in the macroscopic characters of the manuscript text and began his decipherment by transliterating them into Roman letters. A secondary text of 17 different letters resulted. He doubled all but the first and last letters of each section: the secondary text *oritur* would become the tertiary text *or-ri-it-tu-ur.* Any of these groups that contained any of

the letters of the word *conmuta,* plus *q,* underwent a special substitution. The resultant quaternary text was then "translated": Newbold replaced the pairs of letters with a single letter, presumably according to a key, which, however, he never made clear. Newbold regarded some letters of this reduced quinary text as equivalent to one another because of phonetic similarity. When required, therefore, he interchanged *d* and *t,* for example, *b, f,* and *p, o,* and *u,* and so on. Finally, Newbold anagrammed the letters of this senary text to produce his Latin plaintext.

In April, 1921, Newbold announced the preliminary results of his solution according to this method before brilliant and learned audiences. These results stamped Roger Bacon as the greatest scientific discoverer of all time. According to Newbold, Bacon had recognized the Great Nebula in Andromeda as a spiral galaxy, identified biological cells and their nuclei, and come close to seeing the union of the sperm with the ovum. He had therefore to have not merely speculated about but to have actually constructed a microscope and a telescope and used them to make discoveries that anticipated the 20th century. Newbold's cryptanalysis of a caption on a sketch that somewhat resembles a pinwheel and that he took to represent the Andromeda nebula reads in part: "In a concave mirror I saw a star in the form of a snail . . . between the navel of Pegasus, the girdle of Andromeda, and the head of Cassiopeia." Newbold asserted that his solution could not be subjective because "I did not know at the time [of solution] that any aebula would be found within the region thus defined."

Newbold's solution created a sensation in the world of scholarship. Many scientists, though declining to pass upon the validity of the cryptanalysis, which they did not think themselves competent to do, accepted the results with alacrity. One eminent physiologist went so far as to specify that some of the drawings probably represented the columnar epithelial cells with their cilia, drawn to a magnification of 75. The public at large was fascinated. Sunday supplements had a field day. One poor woman came hundreds of miles to beseech Newbold to use Bacon's formulas to cast out the demons that possessed her. The cipher itself drew mixed reviews. Manly, back at 'the University of Chicago, half accepted, half rejected it. "Professor Newbold's theory and system now seem much

more reasonable than they did a year ago when he first explained them to me," he wrote in *Harper's Magazine.* But a writer in *Scientific American Monthly,* J. Malcolm Bird, observed acutely, in relation to the tertiary text of interlocking pairs, as *or-ri-it-tu-ur,* that "Professor Newbold has not in any of his public utterances explained satisfactorily how, in the original encipherment, it is possible to . . . get letter-pairs that interlock as in the above example." In other words, although the system might work in deciphering it did not seem to work in enciphering. Many one-way ciphers have been devised: it is possible to put messages into cipher, but not to get them back out. New-bold's seemed to be the only example extant of the reverse situation. For this and other reasons, Bird rejected the solution.

The excitement simmered down. Newbold went back to continue his solutions; other scholars weighed his conclusions. In 1926, Newbold died. But his working notes, his solutions, and the chapters for the book that he had projected were faithfully edited by his friend and colleague Roland Grubb Kent. In 1928, they were published as *The Cipher of Roger Bacon.* An important French philosopher, fitienne Gilson, later one of the 40 "immortals" of the Academic Francaise, though bewildered by the method, accepted the results; a French specialist in Bacon, Raoul Carton, enthusiastically endorsed both method and results. American and British historians of medieval science were cooler.

In 1931, Manly, who had studied the Newbold method in detail, concluded that it "is open to objections of so grave a character as to make it impossible to accept the results." Warning that these results "threaten to falsify, to no unimportant degree, the history of human thought," he demolished them in a 47-page article. He pointed out that the cipher postulated by Newbold permitted many different "solutions." The encipherer could never be certain that his message would get through correctly; the decipherer would never know whether he was reading the intended message. The chief cause of this flexibility lay in the anagramming process—the one that finally produced the Latin plaintext. Anagramming rearranges letters of one text into another; it is a kind of unkeyed transposition. Often many anagrams are possible: *live, veil, evil, vile,* and *Levi* are all anagrams of the "ciphertext" EILV, each

as valid as the next. As the number of letters involved rises, the possible anagrams increase in geometric proportion. The 31 letters of the angelic salutation, "Ave Maria, gratia plena, Dominus tecum," have afforded thousands of different anagrams, all perfect in spelling, diction, and syntax. One zealot turned out 1,500 pentameters and 1,500 hexameters; another 3,100 anagrams in prose and an acrostic poem; another composed a "Life of the Virgin" in 27 anagrams—all these of the salutation. Newbold tended to anagram Bacon's message in blocks of 55 or 110 letters. How certain could he then be that his anagram was the right one? The answer is that he could not be certain at all.

Manly also showed that the alleged shorthand signs were nothing more than the breaking up of the thick ink on the rough surface of the vellum into shreds and filaments that Newbold had imagined were individual signs. Newbold himself conceded that "I frequently, for example, find it impossible to read the same text twice in exactly the same way." Manly pointed to different solutions from the same text. Finally, he criticized the texts of the solutions themselves on the ground that they "contain assumptions and statements which could not have emanated from Bacon or any other thirteenth century scholar."

How, then, to explain Newbold's cryptanalyzing information that he said he never knew, such as the position of the spiral nebula? The answer is that he must have known it, though subconsciously. Newbold, a scholar of immense erudition who casually learned the Catalan language and read a thousand pages in it in pursuit of a minor point of the solution, must have swept up that detail in his extensive studies and slipped it into the depths of his brain, where it lay hidden from his active mind until the solution drew it forth. No one ever questioned Newbold's integrity; he was a victim, Manly said, "of his own intense enthusiasm and his learned and ingenious subconscious."

The spectacular collapse of the Newbold theory has not deterred other scholars from attacking the manuscript, though it has made them a bit more cautious in publishing their "solutions." In 1943, however, a Rochester, New York, lawyer, James Martin Feely, recklessly exposed to the world—and to its ridicule—a solution that 'makes little sense in Latin and not much more in English: "The feminated, having been feminated, press on the forebound;

those pressing on are moistened; they are vein-laden; they will be broken up; they are lessened."

Two years later, Dr. Leonell C. Strong, a highly respected cancer research specialist, concluded that the Voynich manuscript was the work of one Anthony Ascham, an English scholar of the 1500s and author of an herbal. Strong cryptanalyzed out of the manuscript several texts in alleged medieval English, including a contraceptive formula, by means of a "double reverse system of arithmetic progressions of a multiple alphabet," by which he apparently meant some form of polyalphabeticity. The contraceptive works, and anyone who wishes to prove it may do so, since Strong published it; but he has not seen fit to do the same with his method of cryptanalysis, and it therefore remains unproved and unaccepted. His published texts have been severely attacked on linguistic grounds, and the formula has been explained on the same basis of subconscious knowledge as Newbold's spiral-nebula solution.

There have been many more attempts that did not result in publication because the would-be solvers honestly admitted defeat. Scores of persons have worked at home on the illustrations in the Newbold volume without success. In 1944, from among specialists in languages, documents, mathematics, botany, and astronomy then doing war work in Washington, William F. Friedman organized a group to work on the problem. Unfortunately, by the time they had, working after hours, completed the task of transcribing the text into symbols that tabulating machines could process, the war was over and the group disbanded.

Their preliminary results had the effect of deepening the mystery. For they found that words and groups of words repeat *more* often in the manuscript than in ordinary language. This fact alone differentiates the manuscript from all other cryptograms, for all known cipher systems seek to suppress repetitions, not to intensify them.

What causes this difference? Friedman thought that the manuscript represents a text in an artificial language that has divided all existence into categories, assigned each a basic symbol, and indicated subclasses by additional symbols tacked onto the first. The first artificial language, that of the Scot George Dalgarno, was of this kind. He distributed knowledge into 17 main classes and labeled each

with a consonant: for example, *K* stood for political matters, *N* for natural objects. He subdivided these into subclasses and assigned a vowel to each. Thus *Ke* was "judicial affairs," *Ku* "war." Finer divisions were represented by alternating consonants and vowels. Many other artificial languages of this type have been invented, one by Bishop John Wilkins, who wrote the first book on cryptology in English. Obviously a text in such a language would repeat its "roots" over and over while its suffixes would vary—and this phenomenon is very common in the Voynich manuscript. Friedman planned to test this hypothesis (in which the English cryptologist Brigadier John H. Tiltman concurs) on an R.C.A. 301 computer, but the work did not progress very far.

Another explanation for the great redundancy is that it reflects the many repetitions of pharmaceutical formulas that are likely to occur in an herbal or any medical tract. This is the view of the late Father Theodore C. Petersen, Ph.D., of St. Paul's College in Washington, B.C., an expert in ancient documents who made a 40-year study of the Voynich manuscript. He thought that minute variations in the shape of the characters and in their hooks and other appendages might represent the syllables of a medieval shorthand. He never did collect the statistical evidence he needed to confirm or refute this hypothesis.

Yet men have solved mysteries far more abstruse. Why hasn't anyone unriddled this? The reason, Manly said, is that "the attack has proceeded on false assumptions. We do not, in fact, know when the manuscript was written, or where, or what language lies at the basis of the encipherment. When the correct hypotheses are applied, the cipher will perhaps reveal itself as simple and easy. . . ."

Is it, then, just a gigantic hoax, like the Cardiff giant or the Piltdown man or the fossils of Professor Beringer? Nobody involved with it seems to think so—and this includes those who have been rebuffed by it. The work is too well organized, too extensive, too homogeneous. Nothing repeats larger than a group of five words, whereas in actual hoaxes, such as the fake hieroglyphic papyri sometimes sold to tourists in Egypt, much longer phrases are repeated. Moreover, the words in the text recur, but in different combinations, just as in ordinary writing. 'Even if it were a hoax, there seems to be no point to having made it so long. Most critically, the medieval quasi-

science that was seeking the philosopher's stone and the elixir of life while the manuscript was being written was too credulous to entertain the concept of a hoax.

Voynich died in 1930. His wife, Ethel, kept the manuscript in a safe-deposit box at the Guaranty Trust Company in New York for 30 years, until her death in 1960, aged 96.* Her estate sold it to Kraus. He priced it at $160,000 because he believes that the manuscript contains information that could provide new insights into the record of man. "The moment someone can read it," he said, shortly before the Beinecke Rare Book Library of Yale University obtained it, "this book is worth a million dollars." Others do not think so. They contest the attribution to Bacon, K observing that the manuscript looks much more like a 16th-Tthan a 13th-century work. They feel, as did an American I foundation that turned down Friedman's application for I funds to attack it, that it contains nothing new, that it may be, after all, only some kind of fanciful herbal.

But no one yet knows, and the book lies quietly inside its slipcase in the blackness of Yale's vaults, possibly a time bomb in the history of science, awaiting the man who can interpret what is still the most mysterious manuscript in the world.

## 20. The Anatomy of Cryptology

CRYPTOGRAPHY and cryptanalysis are sometimes called twin or reciprocal sciences, and in function they indeed mirror one another. What one does the other undoes. Their natures, however, differ fundamentally. Cryptography is theoretical and abstract. Cryptanalysis is empirical and concrete.

*Mrs. Voynich deserves a footnote. Her novel, *The Gadfly,* has sold more than 2,500,000 copies in translation in the Soviet Union, •where critics revere her as one of the all-time greats in English fiction. The patriotic romance, a best-seller when it was published in England in 1897, is read by most Russian schoolchildren, forms the subject of Soviet doctoral theses, and has been made into a movie and an opera. The Russians think so highly of it that they paid Mrs. Voynich one of the very few royalty fees they ever gave to an American.

The methods of cryptography are mathematical. "It would not be an exaggeration to state that abstract cryptography is identical with abstract mathematics," declared Dr. A. Adrian Albert. Maurits de Vries, a Dutch statistician and theoretician of cryptology, wrote of cryptography: "The transformations are generally of a simple mathematical nature. E.g. permutations in the set of primary elements (the alphabet); coordinate transformations of lattice points; addition and subtraction in finite rings; linear algebraic transformations. ... A simple example of such a secrecy-transformation is: $y = ax + b$, where $x$ represents a letter of the message; $y$ is the resulting letter of the cryptogram; $a$ and $b$ denote constants which determine this particular transformation. Calculations with the letters are easily carried out after defining a suitable algebra."

Thus the operations and results of cryptography are as universally and eternally true as those of mathematics. Within the "suitable algebra" of the ordinary 26-letter Vigenere, it would be as logically impossible to deny that plaintext *b* keyed with C yields D as to deny that 1+2 =3. And this holds on Mars in the 25th century as equally as in France in the 16th. Different ciphers, like different geometries, yield results that are different but equally valid.

The situation is not at all the same with cryptanalysis. Its methods are those of the physical sciences. They rest, not upon the unchanging verities of mathematical logic, but upon observable facts of the real world. The crypt-analyst must obtain these data by experiment, by measurement. Unlike the cryptographer, who can deduce any enciphering equation in Vigenere from a few initial conditions without recourse to any further experience, the crpytanalyst cannot tell from any number of statements about English which is its most frequent letter. He has to count the letters. The facts may be constants, but they are not logical necessities. They depend upon circumstance, upon reality.

Philosophy offers a useful distinction between statements like those of cryptography and statements like those of cryptanalysis. The statements of cryptography, whose denial would be self-contradictory, are analytic. The- statements of cryptanalysis, whose denial would not be self-contradictory, are synthetic. It might even be said that

cryptography deals with noumena, cryptanalysis with phenomena.

The empirical nature of cryptanalysis appears in its operations. These consist of the four steps of what is commonly called the "scientific method," which scientists apply in attacking problems in the natural sciences. They are: analysis (such as counting the letters), hypothesis (x might be *e),* prediction (if x is *e,* then some plaintext possibilities should emerge), and verification (they do) or refutation (they don't, so x is probably not *e),* either case starting a new chain of reasoning. (This common ground of scientific method between cryptanalysis and other sciences validates such metaphorical statements as "He sought to decipher the history of the earth from layers of rock.")

Within this general format, cryptanalysis operates in two ways, deductive and inductive. Deductive solutions are those based on frequency analysis; they are the general solution for any cipher system. Inductive solutions are those based on probable words or on lucky occurrences, such as two cryptograms with the same plaintext; they are special solutions.

Solutions based on frequency analysis move from a knowledge of letter frequency to an application of it to the cryptogram at hand. Reasoning that flows from the general to the specific like this is deduction. A typical syllogism in the frequency analysis of an English monoalphabetic substitution would have as its major premise, "The most frequent letter in the cryptogram is probably the substitute for *e,"* as its minor premise, "x is the most frequent letter in the cryptogram," and as its conclusion, "x is probably the substitute for *e."* Since all languages have well-defined characteristics of letter frequency, this deductive pattern is known to apply to any cryptogram even before it is inspected. Such a solution is thus a priori in its nature. And because this kind of solution will always work, given enough text, it is the general solution.

Inductive solutions, on the other hand, will work only when certain conditions are fulfilled. Because the crypt-analyst cannot tell whether those conditions are indeed fulfilled until after he has obtained the cryptogram and knowledge of its circumstances, inductive solutions are a posteriori in nature.

If an enemy post radios a message just after it has been

subjected to heavy fire followed by a tank assault, the cryptanalyst might well conclude that the cryptogram contains *bombardment* and *attack* in its plaintext. These are probable words, which he can use to jimmy open the cryptogram. (Common words such as *the, that, and,* and so on, which are probable in all texts because of their high frequency, do not constitute probable words in this sense.) The cryptanalyst's reasoning issues from the numerous specific facts surrounding the message and crystallizes into a single conclusion concerning its plaintext. Such reasoning is inductive. So is the reasoning used in lucky-break, or special-case, solutions. Only after Painvin had noticed the identical bits and pieces of text in two ADFGX cryptograms could he assume that they both had identical plaintext beginnings and thus commence his cryptanalysis (which in this case might better be called a "cryptosynthesis").

Because probable words and special cases enable the cryptanalyst to bring extra information to bear, such solutions display great power and fruitfulness and are often the first to be achieved in new systems. But they are limited to particular situations, and so cryptanalysts seek the deductive general solution of frequency analysis that will always apply.

The realization that cryptography basically constitutes a form of mathematics afforded great insight into the science. It also paved ways to new solutions. In crypt-analysis, the principles of letter frequency gradually expanded to help solve ciphers that at first seemed outside their ambient (such as columnar transposition). When Friedman brought those principles within the broader field of statistics, cryptanalysts could train really powerful new guns upon ciphers. But even this great expansion of knowledge did not reach to the frontiers of cryptanalysis and there confront the phenomenon upon which cryptanalysis rests—the constancy of letter frequency. Shortly after World War II, however, a remarkable new theory emerged that has provided an explanation of that phenomenon and of the whole process of cryptanalysis itself. It has not had the practical effects that Friedman's work has had, but it affords, for the first time, a thorough understanding of why cryptanalysis is possible.

It is called "information theory," rarely, a "mathematical theory of communication." It deals in general with the

mathematical laws that govern systems designed to communicate information. Originating in transmission problems of telephony and telegraphy, it has grown to embrace virtually all information-processing devices, from standard communications systems to electronic computers and servo-mechanisms, and even the nerve networks of animals and men. Its ideas have proved so suggestive that they have been adapted to such fields as psychology, linguistics, molecular genetics, history, statistics, and neurophysiology. Because of this fertility, and because of its potential in helping to manage the information explosion of the 20th century, information theory may eventually rank, *Fortune* magazine has speculated, among the "enduring great" theories of man. The brilliant mind that fathered it also sired its cryptologic applications.

Claude Elwood Shannon was born in Petoskey, Michigan, on April 30, 1916, and was raised in nearby Gaylord, a small town in the north-central portion of Michigan's southern peninsula. He majored in electrical engineering and mathematics at the University of Michigan and there developed an interest in communications and cryptology. At the Massachusetts Institute of Technology, where in 1940 he was awarded a Ph.D. in mathematics, he wrote a master's thesis of such originality that it had an immediate impact on the designing of telephone systems. After a year at the Institute for Advanced Study in Princeton, he joined the staff of the Bell Telephone Laboratories.

"During World War II," he has said, "Bell Labs were working on secrecy systems. I'd worked on communications systems and I was appointed to some of the committees studying cryptanalytic techniques. The work on both the mathematical theory of communications and the cryptology went forward concurrently from about 1941. I worked on both of them together and I had some of the ideas while working on the other. I wouldn't say one came before the other—they were so close together you couldn't separate them." Though the work on both was substantially t complete by about 1944, he continued polishing them until heir publication as separate papers in the abstruse *Bell System Technical Journal* in 1948 and 1949.

Both articles—"A Mathematical Theory of Communica-|tion" and "Communication Theory of Secrecy Systems"— present their ideas in densely mathematical form, pocked vith phrases like "this inverse must exist uniquely" and

expressions like "T^RjCTkR,)-[1]"^!^." But Shannon's terse and incisive style breathes life into them. The first paper gave birth to information theory; the second dealt with cryptology in information-theory terms.

Chief among their new concepts is that of redundancy. Redundancy retains, in information theory, the essence of its lay meaning of needless excess, but it is refined and extended. Roughly, redundancy means that more symbols are transmitted in a message than are actually needed to bear the information. To take Shannon's own elementary example, the *u* of *qu* is redundant because *q* is always followed by M in English words. Many of the *the's* of ordinary language are redundant: persons sending telegrams get along without them.

Redundancy arises from the excess of rules with which languages burden themselves. These rules are mostly prohibitions—"Thou shalt not say 'dese' or 'dose' for *'these'* or *'those'";* "Thou shalt not spell 'separate' as 'seprate' "; "Thou shalt not say 'is' after 'I.'" All such limitations exclude perfectly usable combinations of letters. If a language permitted any permutation of, say, four letters to be a word, such as "ngwv," then 456,976 words would exist. This is approximately the number of entries in an unabridged English dictionary. Such a language could, therefore, express the same amount of information as English. But because English prohibits such combinations as "ngwv," it must go beyond the four-letter limit to express its ideas. Thus English is more wasteful, more redundant than this hypothetical four-letter language.

The rules that lead to redundancy come from grammar ("I am," not "I is"), phonetics (no word in English may begin with *ng),* idiom ("believe" alone may not be followed by an infinitive, only by a clause beginning with "that"). Others come from etymology, in which the derivation of a word has left many now-silent letters, as in "through" or "knight." Still others come from limitations on vocabulary. A teen-ager who uses "swell" to mean what an adult might designate by a dozen different terms of approbation utters speech that is much more redundant, more restricted, less variable, less flexible than the adult's. As Shannon wrote, "Two extremes of redundancy in English prose are represented by Basic English and by James Joyce's book *Finnegans Wake.* The Basic English vocabulary is limited to 850 words and the redundancy is very

high. This is reflected in the expansion that occurs when a passage is translated into Basic English. Joyce on the other hand enlarges the vocabulary and is alleged to achieve a compression of semantic content."

Two other sources of redundancy are of particular importance for their role in determining the frequency table. One derives from the relationships to which human beings refer so often and which language necessarily reflects. These are the relations of one person to another ("the son of John"), of one object to another ("the book on the table"), of an object to an action ("put it down"). English expresses many of these relationships by separate words, called "function words." Pronouns, prepositions, articles, conjunctions are all function words. Some stand for purely grammatical relationships that serve as a kind of linguistic shorthand—saying "I" instead of repeating one's name all the time. Function words mean nothing standing alone. Yet they are among the most common words in English because the relationships they express are so common. In English, only ten of these words constitute more than one quarter of any text: *the, of, and, to, a, in, that, it, is,* and / totalled 26,677 of 100,000 words in a count made by Godfrey Dewey. Inevitably this preponderance will affect the frequency table. *H,* for example, owes most of its occurrences to *the.*

The second source of redundancy stems from the human laziness that favors sounds easier to pronounce and identify. The voiceless stops /ptk/ require less energy to articulate than the corresponding voiced stops /bdg/ and they average twice the frequency of voiced stops in sixteen widely varying languages surveyed by George K. Zipf. Similarly, short vowels are markedly more frequent than long vowels or diphthongs. In the same way, auditors of English, at least, seem to prefer sounds that are easier to identify. Tests made with nonsense syllables show that listeners seldom confuse consonants produced with the vocal organs held in the same position but used in a different manner (such as /ntrsdlz/), but usually fail to distinguish consonants produced with the vocal organs used in the same manner but held in different positions (such as /ptk/). In the first group (the alveolar consonants), the tongue stays at the upper gum ridge but molds or interrupts the breath stream in different ways. In the second group (the voiceless stops), all the consonants block the breath

I

stream and explosively release it, but at different positions of the lips and tongue. It is interesting to note that the easy-to-identify alveolar consonants comprise seven of the eight more-frequent consonants in English, while the two stops that are not alveolar (/pk/) lie well down in the frequency table. Incidentally, this preference for easily distinguishable consonants is one of the few explanations for the arrangement of even a few of the letters in the English frequency table.

All these prohibitions and rules and tendencies help create redundancy. English is about 75 per cent redundant. In other words, about three quarters of English text is "unnecessary." English could theoretically express the same things with one quarter its present letters if it were wholly nonredundant.

Anyone who knows English will know the rules of spelling and grammar and pronunciation that help engender its redundancy, and he will know these rules prior to the receipt of any new text in the language. This is almost tautological: it is only the existence of such rules that makes communication possible. If a hearer interprets "to" to mean "from," he will not understand very much. If he pronounces a written *m* as /v/, a *t* as /s/, and so on, he will not get through to his listeners. These redundant elements, these rules, may be considered the invariant portion of language. They may not be changed without loss of comprehension. But one may say what he wishes as long as he follows them. They are the preexistent mold into which the free-will portion of a communication is poured. Hence the enormous range of texts, from laws to poems, in the same language—which is to say, following the same rules. If one hears the fragment "it's not hard for you to . . .," the redundant elements say that a verb is likely to follow, although the free-will portion makes it impossible to know which one. This same prior knowledge, or, in other words, the redundant elements, detects and corrects errors that arise during the transmission of messages. This is why language tolerates so heavy a burden of redundancy. For example, if a dot is dropped in a telegraphed message in English, so that an i (••) becomes an *e* (•) and "individual" becomes "endividual," the recipient will know that an error was made because English lacks the Sequence "en-dividual." But if the language used were the hypothetical four-letter language, in which all sequences of four letters

were used and therefore all were potentially acceptable in the message, the same dropping of a dot would go undetected. "Xfim," meaning perhaps "come," would be changed to "xfem," maybe meaning "go" and, without redundancy, no alarm bells would ring. (There is, of course, a higher order of redundancy—that mandated by context—which might sound the alarm. If "xfem" meant "green," it would not fit the context. A perfectly non-redundant language can therefore probably not exist, since at least a few basic agreements that a few recurring experiences of the real world will be represented by the same verbal symbols appear to be essential for communication.)

Where the language has no redundancy—as with telephone numbers, where a single wrong digit can lead to a wrong connection—people put in their own redundancy. They repeat the number in giving it to someone. Or, in spelling out names, they say "B as in baby, not v as in Victor." For the greater the redundancy, the easier it becomes to detect mistakes. If a language consisted only of alternations of consonants and vowels, any deviation from that pattern would flag an error.

This detection of errors is the first step toward their correction. And in this correction redundancy again plays the central role. After the recipient of "endividual" has hunted through his memory and his dictionary and found that it does not exist in English, he brings up the sequence "individual," which does exist, from his store of prior information about English, and corrects his message. If the reader of a business letter sees the sequence "rhe company," he will recognize "rhe" as a nonword, will remember that the rules of English often call for a similar-appearing group of letters, "the," before a noun like "company," will perhaps consider that *r* is near *t* on the typewriter keyboard, and then will conclude that "rhe" should be "the."

This process is a first cousin to cryptanalysis.

For cryptanalysts bring to bear in their solutions the same prior knowledge of rules and spelling and phonetic preferences (that is, redundancy) that the ordinary reader does to correct a typographical error. What laymen do with accidental errors, cryptanalysts do with deliberate deformations. Of course a cryptogram is immensely more involved and obscure than an isolated misprint, but it has an underlying regularity that the single random error does not, and

this structure assists and confirms the successive "corrections" that constitute a cryptanalysis.

But how does the cryptanalyst begin in the first place? In correcting a typographical error, all the redundant elements lie in plain view, ready for use. With a cryptogram, they are obscured. The cryptanalyst begins by breaking these elements down to their atomic form—letters. He then compares them to the redundant elements of a language that have been reduced to the same common denominator. In order words, he takes a frequency count of the letters of the cryptogram and matches it against a frequency count of the letters of the assumed plaintext language. (These counts must sometimes be modified by the conditions of the cipher. In polyalphabetics, a count must be made for each alphabet; in digraphics, the count must be of pairs. If the cryptogram is in code, the atomic forms are words, but the same principle applies.)

Having done this, how can the cryptanalyst be confident that the cryptogram's plaintext will have approximately the same frequencies as those of plaintext in general? Why won't the differences in subjects of discussion, in vocabulary, in expression, upset the frequencies? Because the redundant elements of language far outweigh the variable ones. The 75 per cent redundancy in English overwhelms the 25 per cent of "free will"—though this 25 per cent does keep frequency counts from matching one another exactly. The redundant elements in any text converge to make its frequency table. The need in any English text to use "the" frequently ensures that *h* will be a high-frequency letter. English's preference for alveolar consonants will make *n, t, r, s, d,* and / all high- or medium-frequency letters. The language's aversion to *p* and *k* keeps their frequencies low. These redundant elements are fixed and predetermined—necessarily so, if communication is to take place—and hence they stabilize the frequency tables that reflect them.

Shannon's insight, his great contribution to cryptology, lay in pointing out that redundancy furnishes the ground for cryptanalysis. "In . . . the majority of ciphers," he wrote, "it is only the existence of redundancy in.the original messages that makes a solution possible." This is the very basis of codebreaking. Shannon has here given an explanation for the constancy of letter frequency, and hence for the phenomena that depend on it, such as crypt-

analysis. He has thus made possible, for the first time, a fundamental understanding of the process of cryptogram solution.

From this insight flow several corollaries. It follows that the lower the redundancy, the more difficult it is to solve a cryptogram. Shannon's own two extremes of redundancy illustrate this. The last few words of *Finnegans Wake* are these: "End here. Us then. Finn, against! Take. Bussoftlee, mememormee! Till thousendsthee. Lps. The keys to. Given! A way a lone a last a loved a long the." This would interpose distinctly more difficulties to a cryptanalyst than a portion of the New Testament in Basic English: "And the disciples were full of wonder at his words. But Jesus said to them again, Children, how hard it is for those who put faith in wealth to come into the kingdom of God!"

The problem of low redundancy arises in practice with a vengeance when the cryptanalyst is faced with enciphered code. To strip the encipherment from encicode, the cryptanalyst must solve a cryptogram whose plaintext consists of codewords and which may look like KKDYWUKJTPLKJE. . . . This is of very low redundancy because of the more even use of letters, the greater freedom in combining them, the suppression of frequencies by the use of homophones, and so on. But the unavoidable repetitions of orders and reports, the pressure of the redundancy of the language pent within the vessel of the code, and the engineering of codewords so that garbles can be corrected—all these give the underlying codetext a fibrous enough texture for the cryptanalyst to grasp it for solution.

These considerations suggest that reducing the redundancy will hinder cryptanalysis. Shannon himself prescribes operating on the plaintext "with a transducer which removes all redundancies. . . . The fact that the vowels in a passage can be omitted without essential loss suggests a simple way of greatly improving almost any ciphering system. First delete all vowels, or as much of the message as possible without running the risk of multiple reconstructions, and then encipher the residue." Experts who have attacked cryptograms from whose plaintexts only the letter *e* has been eliminated have found that the difficulty of solution increased noticeably. Reducing redundancy is especially effective because it robs the cryptanalyst of one of his chief tools for attack instead of just bolstering the wall of secrecy. Cryptographers of the Italian Renaissance

did this when they ordered cipher clerks to drop the second letter of a doublet, as the second / in *sigillo.*

Such techniques rely upon the cipher clerks' knowledge of their language to supply the suppressed elements of redundancy. Abbreviations likewise may have such low redundancy, may require such an extensive furnishing of information, as *bn* for *battalion,* that they may not only make plaintexts harder to solve, but may themselves function as a rough form of cryptography. Two gossips, for example, may refer to a third party by her initials. They hope that no one within hearing will have sufficient knowledge of the contextual situation to restore the eliminated portion of the name. Much of the Masonic ritual is printed in that form: "Do u declr, upn ur honr, tt u r promptd to. . . ."

Another corollary is that more text is needed to solve a low-redundancy cryptogram than one with a high-redundancy plaintext. Shannon has managed to quantify the amount of material needed to achieve a unique and unambiguous solution when the plaintext has a known degree of redundancy. He calls the number of letters the "unicity distance" (or "unicity point"), and he calculates it by means of a rather complicated formula. This formula naturally differs for different ciphers, but it always includes the redundancy as one of its terms. In his original paper, in which he considered the redundancy of English at only 50 per cent, Shannon found the unicity point for monoalphabetic substitution at 27 letters, for polyalphabetics with known alphabets at twice the period length, for those with unknown alphabets at 53 times the period length, for transposition at the keylength times the logarithm of the keylength factorial.

Shannon has also viewed cryptology from a couple of other perspectives, which, while not as useful as information theory, are enlightening. The first, in fact, is a kind of corollary to the information-theory view.

"From the point of view of the cryptanalyst," Shannon wrote, "a secrecy system is almost identical with a noisy communication system." In information theory, the term "noise" has a special meaning. Noise is any unpredictable disturbance that creates transmission errors in any channel of communication. Examples are static on the radio, "snow" on a television screen, misprints, background

chatter at a cocktail party, fog, a bad connection on the telephone, a foreign accent, perhaps even mental preconceptions. Shannon is suggesting that noise is analogous to encipherment. "The chief differences in the two cases," he wrote, "are: first, that the operation of the enciphering transformation is generally of a more complex nature than the perturbing noise in a channel; and, second, the key for a secrecy system is usually chosen from a finite set of possibilities while the noise in a channel is more often continually introduced, in effect chosen from an infinite set."

When Carl W. Helstrom, author of *Statistical Theory of Signal Detection,* was asked whether the techniques of isolating signals from noise had any relevance to crypt-analysis, he replied: "I suspect that the analogy between the enciphering rule of 'key' and random noise will not prove very fruitful. It seems to me more appropriate to regard the encipherment as a filtering of the original message to produce a transformed version. The 'filter' is a definite transformation rule, but the analyst doesn't know what it is. ... The problem is then to discover the transformation rule, or the nature of the filter, when given the statistics of the input and output. It is like finding the structure of an electrical filter by passing random noise through it and measuring the statistical distributions of the input and output voltages."

Cryptology may also be regarded as a conflict in the sense employed in *The Theory of Games and Economic Behavior* by John Von Neumann and Oskar Morgenstern. As Shannon, who first made the allusion, puts it: "The situation between the cipher designer and cryptanalyst can be thought of as a 'game' of a very simple structure; a zero-sum two-person game with complete information, and just two 'moves.' [A zero-sum game is one in which one contestant's advances are made at the expense of the other.] The cipher designer chooses a system for his 'move.' Then the cryptanalyst is informed of this choice and chooses a method of analysis. The 'value' of the play is the average work required to break a cryptogram in the system by the method chosen."

Cryptology is, by definition, a social activity, and so it may be examined from a sociological point of view. It is secret communication, and communication is perhaps man's most complex and varied activity. It encompasses not just

words but gestures, facial expressions, tone of voice, even silence. A glance can express a tale more sweetly than a rhyme. Basically, all forms of communication are sets of agreements that certain sounds or signs or symbols shall stand for certain things. One must be a party to these preconcerted rules if one wants to communicate.

But all forms of communication are not at all times and all places known. Those who happen to know one system that others around them do not can use it for secret communication. Irish troops sent to the Congo as part of the United Nations force in 1960 spoke Gaelic over the radio, and the U.N. commander, General Carl von Horn of Sweden, called it the best code in the Congo. This is a kind of cryptography by default, depending upon a fortuitous ignorance—a defective cryptography. Effective cryptography deliberately establishes special rules of communication that deny information to those who would otherwise understand the messages.

This withholding of information constitutes the essential element of that which is called "secrecy." All the manifestations of secrecy—hiding places, disguises, locked doors— share the basic idea of not communicating objects or information. Its extreme form is silence (which conjures up an Orwellian nightmare of the extreme form of eavesdropping—detection and interpretation of brain waves). An exhaustive investigation of the concept of secrecy would require, as Maurits de Vries has pointed out, "a complete examination of the relations between individuals and be-tweea groups in our society," because secrecy is the antithesis of communication, and communication—as that which makes man a social being—encompasses all aspects of cultural behavior. Cryptography combines these antitheses into a single operation; a wag might define it as "noncommunicating communication."

The relation between cryptography and cryptanalysis is not logically necessary; it is contingent. One can envision men communicating by secret means with others not even thinking of prying. But in the real world, the cryptanalyst —or more accurately the potential cryptanalyst—comes first. What need for cryptography if no one would eavesdrop? Why build forts if no one would attack? Thus the assumption that someone will attempt a cryptanalysis, no matter how tentatively or incompetently, engenders cryptography.

Experience of the interreaction between cryptography and cryptanalysis has precipitated out certain practical principles. They all refer to time, because all practical matters involving mortal men connect eventually with that one inexorable, irreversible, irretrievable factor.

Time, for the cryptographer, controls a variable relationship. The most general of the cryptographer's principles deals with the sliding ratio between speed and security; as the need for speed in communications increases, the need for security decreases. Early in the planning of a major operation, messages demand great security because the enemy, if he could read them, would have time to prepare countermoves. But in the heat of battle, commanders may use plain language because the enemy, though he intercepts the messages, may not have time to react effectively. This principle arranges a nation's cryptosystems in a hierarchy in which front-line systems are simple and diplomatic systems secure and more complex. "Of each such system," Friedman wrote, "the best that can be expected is that the degree of security be great enough to delay solution by the enemy for such a length of time that when the solution is finally reached the information thus obtained has lost all its 'short term,' immediate, or operational value, and much of its 'long term,' research, or historical value."

The paramount requirement for all cryptosystems is reliability. This means that cryptograms must be decipherable without ambiguity, without delay, and without error. It implies, for example, that cipher machines will be sturdy enough to withstand ordinary abuse so that they will be ready to operate properly when a message comes in. Usually the simpler the system, the more reliable. The requirement excludes from the combat zone ciphers of more than two steps. Any encipherer's errors or garbles should be correctable without having to call for a retransmission. This bans systems in which a single error garbles the message from the point of error on, as in autokey ciphers (such systems are said to have an undesirable error-propagation characteristic). Obviously, if a general cannot rely upon the validity of messages that come out of his cipher machines, the cryptosystem is worse than useless.

Secondary requirements for a cryptosystem are security and rapidity. Which one comes first depends upon the needs of the users. Further down the scale of importance stands

I

the requirement of economy. This rules out any system that requires several men to encipher, makes the ciphertext more than twice as long as the plaintext, or is too complicated or expensive to manufacture or distribute.

In addition to these general requirements, military and diplomatic cryptosystems must meet two specific ones— both first enunciated by Kerckhoffs. The first rests upon the almost universal employment of telegraphy or radio-telegraphy for military and diplomatic communications. No system is acceptable whose cryptogram characters cannot be sent in Morse code; excluded are squares, angles, crosses, or other designs. The second rests upon a working assumption of military cryptography: that the enemy knows in general how a cipher works. Secrecy must depend upon the keys used. No method is acceptable that does not accede to this requirement, that does not provide for both a general system and specific keys.

For the cryptanalyst, time's demands remain fixed. Always at his back he hears time's winged chariot hurrying near. He seeks to get out his solutions as quickly as possible. It is probably true that a message will always have some historical value, but that is small comfort to a commander who does not get a cryptanalysis that would have warned him of an enemy attack until after the attack is under way. The factors that affect the time required to solve cryptograms—aside from external factors, like the speed of sending the intercepts back to the cryptanalyst— are the strength of the system, the soundness of the regulations for its use, how closely the cipher clerks follow those regulations, the volume of text, the size and skill of the cryptanalytic organization, and the amount and character of collateral information.

Bringing skill into the picture raises the question of whether cryptanalysis is a science or an art. It is both. On the one hand, cryptanalysis—or, more properly in this context, cryptanalytics—is an organized body of knowledge. It studies and controls phenomena. Its whole spirit is scientific, but that of an applied science, like engineering. On the other hand, cryptanalysis—here meaning the steps performed in solution—clearly depends upon personal ability. Some cryptanalysts are better than others. In this sense, cryptanalysis is an art. So, in this sense, is any human activity that demands a certain aptitude for its superior practice. Yardley said that outstanding crypt-

analysts were gifted with "cipher brains," and rather glamorized the faculty, but in fact "cipher brains" are just the cryptologic manifestation of a general characteristic— talent in a given field. Who possesses "cipher brains" and why, however, raise complicated questions.

Human knowledge not only cannot answer them now, it does not even understand how the mind performs the basic psychological operation of cryptanalysis—pattern recognition. How the brain can supply the missing letters to a fragment of plaintext which it has never before seen resembles such problems as how one can read words in a handwriting one has never seen or recognize a piece of music as Mozart's even though one has never heard it before. These problems remain among the still unsolved ones of psychology and biochemistry, as convoluted as the cerebral cortex and molecular chains which may hold the answer.

If the psychological roots of cryptology remain obscure, the biological roots are clear. Those roots reach back through the eons to the first protozoa struggling for life in the warm seas of the primordial earth. For cryptography and cryptanalysis, though they are highly sophisticated technologies, retain at their inmost cores, like chromosomes that determine their heredity, the most primitive of functions.

Cryptography is protection. It is to that extension of modern man—communications—what the carapace is to the turtle, ink to the squid, camouflage to the chameleon. Cryptanalysis corresponds to the senses. Like the ear of the bat, the chemical sensitivity of an amoeba, the eye of an eagle, it collects information about the outside world. The objective is self-preservation. This is the first law of life, as imperative for a body politic as for an individual organism. And if biological evolution demonstrates anything, it is that intelligence best secures that goal. Knowledge is power. In an atmosphere of competition, it may exist in two modes: mine and mine enemy's. All organisms attempt to maximize the former and minimize the latter. Cryptography and cryptanalysis exemplify the two modes. Cryptography seeks to conserve in exclusivity a nation's store of knowledge, cryptanalysis to increase that store. But knowledge alone is not power. To have any effect it must be linked to physical force. Cryptology, like the services of supply and transportation and administration, aids the fighting troops that constitute a main element of

national power. Nations use that power to advance their political and social goals. Cryptography and cryptanalysis are means to those ends. And that is their position in the ultimate scheme of things.

Even when the ends that they serve are purely defensive in regard to other nations, there exists a difference in morality between the means of cryptanalysis and such means as armies and navies. The latter are honest and above-board, open deterrents to aggression; they are like strong men armed. Cryptanalysis is itself an aggression— often a preventive one, to be sure—but still an aggression, a trespass. Moreover, it is surreptitious, snooping, sneaking; it makes its government hypocritical. It is the very opposite of all that is best in mankind. It shatters the highest ethical precept: to do unto others as we would have others do unto us.

Is it, then, ever morally justified? It is. A single act can be both moral and immoral, depending on circumstances. Killing is permissible in self-defense. So is cryptanalysis. In war, of course, cryptanalysis can look like a positive good, especially when it saves lives. Even in peace, cryptanalysis may be a form of self-defense. It can warn of hostile intent and enable the government to preserve life and liberty, without which there is no doing to others of any kind. But when a nation is not threatened, it is wrong for it to violate another's dignity by clandestine pryings into its messages, just as it is wrong to indiscriminately tap telephone lines or invade the privacy of a man's castle. That is why it is indefensible for the United States to read the messages of friendly nations like Norway, Britain, or Peru.

Even when justified, cryptanalysis remains an evil, and it goes against the American grain. Ever since July 4, 1776, the United States has stood for morality and integrity, in international affairs as in domestic, in the Fourteen Points as in the Emancipation Proclamation. It is this stand that, in large measure, makes America great. Cryptanalysis therefore poses a much greater problem for the United States than for other nations. It perhaps reflects this concern that the United States places her national crypt-analytic agency within the Defense Department, where it belongs in ethical terms, while Great Britain puts hers in the Foreign Office, where it belongs in a practical way.

Only once has cryptanalysis been treated as the sin

against morality that it is: in 1929, before Hitler and the Japanese militarists, with no nations potentially dangerous to the United States and self-preservation not at issue, Henry L. Stimson closed Yardley's Black Chamber. Even though it was done at a time when the United States could afford it, the decision was a profoundly moral one, and it marched in the center rank of American belief. Was it soft-headed, unrealistic? No. Idealism is the ultimate realism. Ideas of truth and justice always eventually triumph. Mankind can learn. America's whole history shows this, as does humanity's ascent from barbarism. The growth of wisdom and morality—urged on in these present times by the very real danger of total annihilation—may some day lead mankind to beat its swords into plowshares. When it does, it will no longer need cryptanalysis, and will dismantle organizations like N.S.A. and the Spets-Otdel. Their nonexistence then will testify to a true peace on earth. And may such be their glorious destiny!

## Suggestions for Further Reading

IF YOU ENJOYED reading about codes and ciphers and want to learn more about them, the following list may guide you. It includes only works in print in English; libraries will have others.

First, of course, is the unabridged version of this book. Though it adds but little to the individual episodes as printed here, it enriches the background with other stories and technical details, and cites sources. It is published under the same title by the Macmillan Company, 866 Third Avenue, New York, New York 10022, 1164 pages, $17.50.

To solve cryptograms, join the American Cryptogram Association. This worldwide organization of mutually helpful amateur cryptologists publishes a small magazine every other month with cryptograms for solution and articles on how to solve them. Dues are $3.00 a year; the treasurer is Miss Edna Bickley, 312a West Jackson, Mexico, Missouri 65265.

Two books describe the standard cipher systems and how to solve them. Abraham Sinkov's *Elementary Crypt-analysis* (Random House, 1968, 189 pages) is very clear and effectively relates the techniques to the underlying mathematics. Helen F. Gaines's *Cryptanalysis* (1939, reprinted Dover, 1956, 237 pages) covers more ground but is less understandable.

Other works deal with aspects of the subject. Barbara W. Tuchman recounts the political effects of the most important cryptogram solution in history in *The Zimmermann Telegram* (1958, reprinted Macmillan, 1966, 244 pages). Ladislas Farago's *The Broken Seal* (Random House, 1967, 441 pages) tells about the development, theft, and solution of Japanese cryptosystems before Pearl Harbor. William F. and Elizebeth S. Friedman's *The Shakespearean Ciphers Examined* (Cambridge University Press, 1957, 303 pages) is a witty expose of the kooks who "decipher" false authorship claims of Francis Bacon from Shakespeare's plays. And Raymond T. Bond has collected sixteen of the

458

better short stories involving a cryptogram, including those by Poe, A. Conan Doyle, Agatha Christie, and O. Henry, in his *Famous Stories of Code and Cipher* (1947, reprinted Collier Books, 1965, 383 pages). For youngsters, the following are the best of the many books in print: Sam and Beryl Epstein, *The First Book of Codes and Ciphers* (Franklin Watts, 1956, 62 pages), for grammar-school ages; Herbert S. Zim, *Codes arid Secret Writing* (William Morrow, 1948, 154 pages), for the junior high school level; and James Raymond Wolfe, *Secret Writing: The Craft of the Cryptographer* (McGraw-Hill, 1970, 192 pages), for the high school level.

# Index

0075 code/134, 137, 139, 140, Ame, C., 248
142, 143, 145, 148 13040 code, 137, 143, 144, 148,171
A-3 scrambler, 294-298
Abbasi, A., 374
*ABC Code,* 278
Abel, R., 371-372, 376
*Acme Code,* 278
ADFGVX system, 158-164, 167,
442
ADFGX, 158-161, 165 "Adventure of the Dancing
Men, The," 416-420 Advertisements, personal, in
newspapers, 414-416 A.E.F. *See* American Expeditionary Force A.F.S.A. *See* Armed Forces
Security Agency Akin, S. B., 320 Aktiebolaget Cryptograph, 211 Aktiebolaget Cryptoteknik,
211
Albert, A. A., 440 Alberti, L. B., 90-95, 98 All-purpose cipher, 401-402 Alphabet cipher, xii Alphabetical
Typewriter (cipher machine.) *See*
PURPLE Amateurs, 388-389, 402-408
*See also* inventors
American Black Chamber. *See* Black Chamber
*American Black Chamber, The,* 179-181
American Cryptogram Association, 410, 411-412
American Expeditionary Force, 156-157
American Indian languages, 289-290
American Telephone and Telegraph Company, 193-199, 202-203, 294, 295, 409
Amjadi, M., 374
AN-103, 325
Anderson, W. S., 3, 340
Ango Kenkku Han, 322
Arabs, 80-82
Argenti, G. B., 86
Arisue, S., 328
Armed Forces Security Agency, 379-380
Army Security Agency, 15, 319,381
*Artha-sastra,* 71
A.S.A. *See* Army Security Agency
Atbash, 72-73, 292
Atlantic, Battle of, 244-245, 268-272
*Atlantis,* 243
Atlas computer, 394
A. T. & T. *See* American Telephone and Telegraph Company
461

Atterbury, F., 107-108 Augustus Caesar, 77 Australia, 266 Austria, 128-129
*See also* Dechiffrierdienst; Geheime Kabinets-Kanzlei
black chamber, 104 Austria-Hungary, 128 Authenticators, 315 Autokeys, 97-98, 409, 453 Automated cryptography, 197 "Automatic cryptography,"
198
B section, 245-246 Babbage, C., 406, 415 Babington, A., 87-89, 417 Babylonia. *See* Mesopotamia Bacon, Sir Francis, 166, 430,
432, 458 Bacon, R., 430-432, 434-435,
436
Bacon-Shakespeare controversy, 184-185 BAMS code, 243, 325 Band-shift, 292-293 Band-splitting, 293, 294 Baudot code, 195 Barber, R. T., 337 Barne, L, 412 Barne, W., 412 Baudot code, 194-195, 261 Baudot, J. M. E., 195 Bazna, E., 228 B-Dienst, 241-245, 264, 268 Belaso, G. B., 96-98 Bell, Edward, 146-147 Bell Telephone Laboratories,
443 *Bentley's Complete Phrase*
*Code,* 278 Beobachtung-Dienst, 241-245,
264, 268
Bergenroth, G. A., 424-^28 Bernstorfi, J. H. A., von, 134-
153 *passim* Berthold, H. A., 156-157
Bestuzhev-Ryumin, A., 341 Beurling, A., 258, 261-262,
663
Bible, 72-73 Bibo, Major, 230-231 Bigram, definition, xiii Bird, J. M., 435 BLACK code, 249, 254 Black chambers, 104-106,109, 274, 341
American, 6, 173-179, 191,
192, 457
Bletchley Park, 263-264 Boki, G. L, 359-360, 362 Bond, R. T., 549 Book cipher, 186-187 Bratton, R. S., 30 Braune Blatter, 225 Breon, W., 279-280, 286 Brooke-Hunt, G. L., 172 Brotherhood, F. M., 1-2, 11 BROWN code, 323 Browne, Sir Thomas, 432 Bryant, H. L., 2-3, 4, 47 Bullock, F. W., 317 Bureau du Chiflre, 159 Burke, J. P., 390 Busch, H., 271 Business codes, 422-423 Byrne, J. F., 408-410
C-36, 212 Cabinet Noir, 111 Cablegrams. *See* Commercial
codes Cables, German transatlantic,
cutting of, 129 Caesar alphabet, 77 Caesar, J., 77 Caesar substitution, 77, 95,
292, 354, 414, 415 Canada, 183, 266 Canaris, W., 249 Carbonari, 419 Cardano, G., 146 Cardano grille, 281, 283 Cartier, F., 159 Cave, R., 46

Cavendish-Bentinck, V. F. W.,
266
C.B., 319-320, 322 Censorship, U.S., 274-289 Central Intelligence Agency, 378, 379, 382, 383, 384, 398
Chamber analysis, 166, 257 Chaocipher, 409, 410 Chase, P. E., 121-122 Chaucer, G., 171 Checkerboard, 76,
121-122, 186, 343, 357-359, 368, 369, 376 *See also* ADFGVX; Straddling
checkerboard
Chetardie, Marquis de la, 341 Chiffrierabteilung, 233-237 CHI-HE, 309 Childs, J. R., 172 China, 71, 281 Church
registers, 312 Churchill, W. L. S., 131-132,
244, 267-268,297-298 C.I.A. *See* Central Intelligence
Agency
Ciano, G., 248, 249 Cicero, operation, 228-230 Ciphers, xii, xiii-xiv all-purpose, 401-402 *See also* codes;
Monoalpha-betic substitution; Poly-alphabetic substitution; Transposition
Cipher alphabet *See* Alphabets Cipher devices cipher reel
*See* cipher disks; cipher machines; grilles; multiplex system; skytale Cipher disks, 92-94, 403 Cipher machines,
167, 339,
401, 402, 453
*See also* A.T.&T.; Cipher disks; csp-642; Enigma; Hagelin machine; Jefferson cipher; M-94; M-134; M-138; M-
209; PURPLE; Siemens & Halske; SIGABA;
SIGTOT; Wanderer Werke Ciphertext, definition, xiv Ciphony, 291-298 Clark, H. L., 24 Clausen, H., 379
Clausen, M. G. F., 368-369 Cleartext, definition, xv Cleaves, H., 223 Code, 71, 112, 126, 167, 173-176, 216,
219, 259, 290-291, 330-331, 354, 356, 362-363 commercial, xiv, 111, 130,
278
definition, xii-xiv enciphered. *See* Enciphered
code
one-part, defined, xiii solution of, 139-140, 143-
144, 218-219, 223 two-part, defined, xiii *See also* 0075; BROWN; KRU; LA; under individual names Code and
Cipher Compilation
Section, 191 Code and Signal Section, 12,
192, 207, 302
Codebreaking, definition, xv Codegroups, definition, xii-xiii Codenames, 266-268 *See also* under individual
codenames
Codenumbers, definition, xii Codetext, definition, xiv Codewords, definition, xii Coincidence, theory of, 189
Collins, S. W., 286 Combat Intelligence Unit, 8,
10,12,16,35,300-314 Communications intelligence,
xv Communications Intelligence
Summary, 37
Communications security, xv "Communication Theory of Secrecy Systems," 443-444

Computers and tabulators,
393-395
COMSEC, 387-390 Consolidated Exporters Corporation, 421-422 COPEK, 30,45,303,311 Coral Sea, Battle of, 304-305, 310
Corbiere, A., 107 Corderman,W. P., 317 Cory, Mr., 33 Council of Ten, 83 Craig, M., 14 Cramer, G., 413 Cryptanalysis as a physical science, 440-
442 becomes a major element of
intelligence, 165 becomes most important element of intelligence, 339-340
becomes specialized, 166 coining of term, 190 contrasted with cryptography, 154, 410, 439-441, 452, 455 definition, xv linquistic bases of, 81-82 machines for. *See* Robot cryptanalysts; Computers and tabulators mathematization of, 339
methods of, 441-442 physical nature of, 440 pleasure of, 410-411 science or art, 454—455 time element in, 453-454 *See also* Cryptanalytics;
Cryptology Cryptanalytics, 454 Cryptanalyze, definition, xv Cryptogram, definition, xiv *Cryptogram, The,* 411
Cryptography as noise, 450-451 contrasted with crypt analysis, 154, 410, 439-441, 452, 455
definition, xi hierarchy of systems, 17 machines for. *See* Cipher
machines
mathematical nature of, 440 mechanization of, 339 pleasure of, 410 practical principles, 453-454 spontaneous origins of, 77 time element in, 453-454 *See also* Cryptology; Cryp-
tophony; Steganography Cryptology Arabs create, 80 as a black art, 79 biological roots of, 455 definition, xv future of, 400-402 game theory, 451 literacy's effect, 77 morality of, 178 ontology of, 455-456 permanent embassies' effect, 83
psychological bases of, 455 radio's effect, 153-155 sociology of, 451-452 telegraph's effect, 111-114, 154-155 U.S. takes world lead in,
191 West takes lead over East
in, 92 World War I's effect, 165-
167 World War IPs effect, 338-
340 *See also* Cryptography;
Cryptanalysis
Cryptophony, definition, 291 csp-642, 326 Cuneiform cryptography, 72
Dahlerus, B., 214-215 Dalgarno, G., 437-438 Damm, A. G., 210-212, 256, 339

Dancing Men cipher, 416-420 Dasch, G., 285 Dato, L., 91 David, A. L., 271 Deceptions and dummy traffic, 36-37
Dechiffrierdienst, 350, 356 Decipher, definition, xv Decode, definition, xv Decipherers, British, 107-111 Deciphering Branch, 109-111 Deductive solutions, 441-442 Dee, J., 431-432 De Grey, N., 134-135, 138, 140-141, 149, 265 Department of Communication, 263-264, 265-266 De-Scrambler, 293 Deubner, L., 351-352, 353,
355
Deutsche Reichspost, 295-298 De Vries, Marquis, 440, 452 Dewey, Godfrey, 445 Digraph, definition, xiii Digraphic substitution, 118-
121, 228 Direction-finding, xvi, 9, 132,
269-270
Disk, cipher. *See* Cipher disks Donitz, K., 237, 241 Doolittle, J., 307 Double transposition, 238 Doud, H. S., 11 Doyle, A. C., 416-420 Draemel, M. F., 207, 306 Dulles, A. W., 379, 398-399 Dulles, J. F., 399 Dummies. *See* Fake messages;
Nulls
Dunning, M. J., 46 Dyer, T. H., 45, 300-303, 312,
330, 333
Eckhardt, H. von, 143, 149-
150, 171
Edgers, D., 27, 47 Eisenhower, D. D., 274 Electric Code Machine, 207
Electronic security, xv *Elements of Cryptanalysis,*
191
Encicode, definition, xiv Encipher, definition, xiv Enciphered code, 175, 216, 219, 221, 230, 362-363, 367, 422-423, 449 definition, xiv invention of, 94 solution of, 131-132 *See also* J codes PA-K2; Schliisselheft Encode, definition, xiv England, 86-90, 106-11, 129, 177, 224, 248, 239, 242-245, 395, 398 *See also* Bletchley Park; Decipherers; Deciphering Branch; Department of Communications; M.I. 1 (b); M.I. 8 Enigma, 6, 21, 210, 211, 237,
238, 240, 271, 367 Eno, A. L., 194 Epsilon Eridani Epstein, S. and B., 458 "Erring Siamese," 77-78 Euler, L., 406 Evans, A. R., 328 Ewing, Sir Alfred, 129-132, 133
F and p inks, 169-170
Fabian, R. J., 12, 26, 37, 301, 302,308,312
Fabyan, G., 184, 185, 433
Fake messages, 246-247
Fallacy of key size, 407
Family codes, 283
Farago, L., 458
Federal Bureau of Investigation, 276, 286, 287, 372, 378
Federal Communications Commission, 34, 42
Feely, J. M., 436-437
Fellers, B. F., 250-254 *passim*

Fellgiebel, E., 232-233, 236-
237
Fenner, W., 235 Fernmeldeaufklarung, 238,
253-254 Field ciphers
origin of, 112-113,166
principles of, 126-127, 453-
454
Figl, A., 128, 227-231 *passim* Fingerprinting apparatus,
radio, 386 Finland, 258, 364 Finnegan, J., 310 "Fists" of radiotelegraphers,
31 Five-numeral system. *See* JN-
25 Five-Power Treaty, 176, 177,
181
Flag officers' system, 8,45, 301 Fleet Radio Unit, Pacific
Fleet. *See* FRUPAC Fletcher, F. J., 304 Foote, A., 368-369 Forschungsamt, 215, 224-226,
227, 228, 230, 232 Forschungsanstalt, 295-298 Fractionating ciphers, 121-122
*See also* ADFGVX France, 83-86, 101-104, 106, 110, 111, 172, 224, 260-261, 341, 395, 397, 398
*See also* Bureau de Chiffre;
Service du Chiffre Franz, W., 236 Freemasons' cipher, 413-414 Frequency of letters, analysis
of, 81-83, 91, 167, 339,
441-442
Frequency counts, 81-82 Friedman, E. S., 185, 458
rumrunning solutions, 420-
422 Friedman, W. F., 183-192
and Yardley, 179, 183
as teacher, 190
at Riverbank Laboratories, 185-187, 190
Baconian studies, 184-185
characteristics, 183-184
contributions to cryptology, 339
early life, 183-185
Hindu solutions, 186-187
in G.2 A.6, 188
in Signal Corps Code & Cipher Compilation Section, 190-192
in S.I.S., 6, 192
*Index of Coincidence,* 189, 190
interest in cryptology, 185
inventions, 190
nervous breakdown, 26
Pletts machine solution, 187
PURPLE solution, 1-2, 11, 24-25, 191, 213
Voynich manuscript, 437
writings, 188-190, 458 Friedrichs, A., 217, 219, 223,
221 FRUPAC, 311-312, 314-315,
331-333 Fuchs, K., 371 Funkaufklarungsdienst, 240-
241
0.2 A.6 155-157, 189 Gaines, H. F., 458 Gallery, D. V., 270-271 Gallup, E. W., 185 Gamba, V., 246 Game
theory, 451 Gamma epsilon, 133 Gamma u, 133 Gardner, N., 275 Gaussin, J., 197 Geheime Kabinets-Kanzlei,
104-106, 111 General system, xvi, 127 Geometrical systems, 281, 283 Germany, 129, 134-153, 156-161, 177,
237-245, 261-

Germany (continued)
263, 271, 364-365, 366-367
0075 (German code), 134, 137, 139, 140, 142, 143, 145, 148 13040 (German code), 137,
143, 144, 148 Reichsicherheitschauptamt,
226-231 Wehrmachtnachrichtenver-
bindungen, 232-233 *See also* 0075; 13040; B-Dienst; Chiffrierabteil-ung; Forschungsanstalt; Forschungsamt;
Funkauf-klarungsdienst; OKH; OKL; OKM; OKW; Pers z; S.D.; Sonderdienst Dahlem
Gestapo, 225, 226 Gherardi, L., 248-249 Gifford, G., 87-88 Glavnoye, Razvedyvatelnoye Upravlenie, (G. R. U.)
368 Goggins, W. B., 315 "Gold-Bug, The," 388, 416 Gorgo, 75 Goring H., 215, 224-225,
227
GRAY code, 322, 333 Great Britain. *See* England Greece, ancient, 73-76 Grille, Cardano, 281, 283 G. R. U.
*See* Glavnoye Razvedyvatelnoye Upravlenie
Guitard, M., 159, 163-164 Gusev, 361 Gyld6n, O., 256 Gylden, Y., 256-258, 259
Hagelin, B. C. W., 210-214,
339
Hagelin machines, 210-214, 237, 400, 406, 422
*See also* M-209 Hague Convention articles of
war, 43
Hall, W. R., 133-134, 141-142, 146
Hamilton, V. N., 397
Hancock, C. B., 340
HARUNA, 39, 40, 41, 67
HATO code, 6, 38
Hayhanen, R., 376
Hebern, E. H., 191, 193, 206-210, 339
Hebern Electric Code Inc., 207-210
Hebrew ciphers, 72-73
Heeresnachrichtenwesens, 237
Helstrom, C. W., 451
"Hermit metamorphosing letters," 78
Herodotus, 74-75
Hieroglyphic cryptography, 68-70
Hill, L. S., 339
Himmler, H., 225, 226-227
Hindenburg, P. von, 346, 347, 352
Hindus' ciphers, 186-188
Hira gana, 310
Historians, 423-428
Hitchings, O. J., 301
Hitler, A., 210, 223-224, 225, 229, 296
Hitt, P., 199, 203, 409
H.N.W. *See* Heeresnachrichtenwesens
Hoffmann, A. B., 351
Hoffmann, E., 216
Hollerith tabulating machines, 318
Holmes, W. I., 306, 331
Holmes, S., 416-420
Holtwick, J. S., Jr., 22, 305
Roman, W. B., 403
Homer, 73-74
Homophones, xii, 80
Hoover, H., 177-178
Hoover, J. E., 287
Hornbeck, S. K., 181
Homer, E. W., 289
Hottl, W., 227-231, 248
Houdini, H., 411
House, E. M., 137-138, 168

Huffduff, 269-270
Hull, C., 4, 29, 32, 33, 46
Hungary, 230-231
*See also* Austria-Hungary Huttenhain, E., 236
*1.1.,* 332
I.B.M. *See* International Business Machines Corporation
Ibn ad Duraihim, 80-81
I.D., 132
Identification-friend-or-foe system, (I.F.F.), 390
*Iliad,* 73-74
*Index of Concidence and Its Applications in Cryptography,* 189, 190
India, 71-72
Indian languages, 289
Indians, American, 289-290
Inductive solutions, 411-442
Information theory, 442-450
moo DENPO, 33-34, 56
Institute for Defense Analyses, 387, 389-390
Intelligence Bulletins, MAGIC, 28-29
Interception, xv, 13-15 154-
155, 391-392
*See also* Mail opening; Traffic volume; Wiretapping
International Business Machines Corporation, 394 Machines, 300, 302, 305, 308, 318, 320, 326, 332-333
International Code Machine Company, 207
International Communication Laboratories, 203
International Telephone and Telegraph 203
Inventors, 388-389, 402-408
Inversion, 292
Inverter, 292, 294
Invisible inks, 169-170, 275, 276, 284-287
Isomorphic cryptograms, 23 Italy
Servizio Informazione Mili-
taire, 246-248 Servizio Informazione Se-
greto, 245-246 *See also* B section; Sezione
5; Sezione 6; Venice Ito, S., 46
j series of Japanese diplomatic codes, 15, 19-20, 39, 220 J19, 39
Ja, 175
Janssen, H. P. M., 282
Japan, 1-68, 173-175, 266, 273-274, 301, 303, 307, 310-311, 322, 330, 332
*See also* Ango Kenkyu Han; Tokumu Han
"Japanese Diplomatic Secrets," 181
Jargon code, 281-282
Jefferson cipher, 114-116,
191, 222
*See also* csp-642; M-94; M-138
Jerdan, W., 404
JN25, 8, 12, 45, 301, 303, 307, 311-312, 314, 332
jN25b, 8, 12, 303, 307
JN25c, 303, 311
Johnson, L. B., 400
Joyce, James, 408-410, 444-445
jp, 176
Kakimoto, G., 325 *Kama-sutra,* 72 Kameyama, K., 30, 46 Kasiski examination, 199-200 Kasiski, F. W., 122-124
Kasiski solution, 198, 199-200 Kata kana, 173-174, 310 Kautilya, 71

Keitel, W., 233 Kempf, S., 233 Kennedy, J. F., 328-330 Kerckhoffs, 124-125, 126-
128, 454 Kerckhoffs superimposition,
127-128, 200, 205 Kesselring, A., 238, 239 Kettler, H., 233 Keys
definition, xiv
general system, 127
generation of, 401-402
orgin of, 96-97
*See also* Autokeys; Running
keys
Keynumber, definition, xiv Keyphrase, definition, xiv Keyphrase cipher, xiv Keyword, definition, xiv
Kharkevich, 361 Khnumhotep II, 69 King, E. J., 307 Kinsey, A. C., 413 Kircher, A., 430 Kita, N., 16
Knatchbull-Hugessen, Sir
Hughe, 228 Knights of the Golden Circle,
413
Knispel, H. K., 271 Knox, F., 4 Koch, H. A., 210 Kowalefsky, J., 175, 322 Kramer, A. D., 3, 4, 13, 47-48, 54-
55
*See also* OP-20-G Kraus, H. P., 428, 439 Kripo, 226 Krivosh, R., 361-362 Krivosh, V., 361-362 Kroger, H. and
P., 372 KRU codes, 155-156 Krug, H. G., 218 Kühn, B. J. O., 39, 47, 66-67 Kullback, S., 192, 318, 329,
385 Kunze, W., 216, 218, 223-
224, 301, 339
LA, 17-18, 38, 40, 45, 46 Langlotz, E., 216 Lanphier, T. G., Jr., 336-337 Lansing, R. L., 148-149 Lasers, 402
Lasswell, A. B., 46, 334 Layton, E. T., 36-37, 308-309, 311
**LEB KAMAI, 72**
Lesson, J., 412
Letter frequency, 442, 446,
448 *See also* Frequency analysis
Letters of the alphabet, characteristics of, 81-82, 91
Lexicography, 81
*Lexington,* 304
Literature of cryptology, 416-
420, 457-458 American, 189, 190
Livesey, F., 172, 175
"Lucy" network, 368, 370
Ludendorff, E., 161-164, 346-347, 352-354
Ludwig, K. F., 276
Luftnachrichten, 240
Luning, H. A., 276
Lynn, G. W., 13
M-94, 191
M-134, 317
M-138, 222, 254, 323
M-209, 213, 214, 238-239,
317, 338, 363 MacArthur, D., 30, 303 McCollum, A. H., 3, 4 Mackay Radio & Telegraph
Company, 53 Mackensen, A. von, 158, 352-
354 Mackensen, H. G. von, 248,
249
*Magdeburg,* 131 MAGIC, 3, 393
distribution, 28-29
importance of, 29-30
translation, 27-28

MAGIC *(continued)*
*See also* J codes; PURPLE;
OP-20-o; S.I.S. Magic, 79, 84, 86 Magnus, A. von, 150 Mail opening, 104, 108-109 Manly, J. M., 169, 171, 179, 433, 435-436, 438 Mannerheim, C., 363 Marci, J. M., 430 Marshall, G. C., 14, 28-29, 30, 57, 58-61, 312-314 Martin, W. H., 390-391, 396-397
Mara code, 331 Mary, Queen of Scots, 86-90, 417
Masking system, 293 Masons, 413 "Mathematical Theory of Communication, A," 443-444 Mathematics, 339, 440, 442
*See also* Statistics Mauborgne, J. O., 198-199, 301
as Chief Signal Officer, 7, 24
cryptologic highlights, 7
invents unbreakable cipher, 198-199
May, A. N., 371 Mayfield, I. S., 16, 40 Mellenthin, F. W. von, 365, 366
Menet Khufu, 68 Mesopotamia, 72 Mexican microdot ring, 288 Meyer, A., 207 M.I. l(b), 172, 187, 264 M.I. 8 (Great Britian), 264 Mi-8 (U.S.), 168-173 Microdot, 287-289 Middle Ages, 78-79 Mid-Pacific Strategic Direction-Finder Net, 9, 11 Midway, Battle of, 309-310, 311-314 Minckler, R. W., 11
Mitchell, B. F., 390-391, 396-397
Mitchell, J. W., 336 Mobasheri, J., 374-376 Monalphabetic substitution, 77-79, 406, 407, 412, 413, 417, 444-445
definition, vii
solution of, 81-83
*See also* Atbash; Caesar substitution; Checkerboard
Montdidier, Battle of, 164 Montgomery, B., 256 Montgomery, W., 134-135, 138-139, 263
Moorman, F., 156, 157, 409 Morehouse, L. P., 197-198 Moreo, J. de, 84-85 Morgenstern, O., 451 Morikawa, H., 322, 325 Morimura, T. *See* Yoshikawa, T.
Morse code, 454 Morse, S. F. B., Ill Moyzisch, L. C., 229 Muller, H. K., 221 Multiplex systems. *See* CSP-642; Jefferson cipher; M-94; M-138
Multiplexing, 194 Murphy, R., 221-222 Murray, A. A., 13 Music, 301 Myzskowski, E., 403
Nachrichten-Verbindungswesen, 240 Napoleon, 342 National Puzzlers League, 411 National Security Agency, 378-400
budget, 383-384
building, 381-382
cryptanalysis, 392-398
duties, 380-381
founding, 380

National Security Agency (continued)
organization of, 385-387, 390-391
overseas branches, 382
results, 396-400
security in, 383-385
size, 382 Navahos, 289-290 Naval disarmament, conference for, 176-177 Nebel, F., 161 Neumann, J. von,
451 New York Cipher Society,
410, 412
Newbold, W. R., 433-436 Newspapers, personal advertisements in, 414-415 Nigeria, 77
Nihilist cipher 344, 368 Nimitz, C. W., 303, 304, 310,
311, 312, 334, 335, 337 97-shiki O-bun In-ji-ki, 21, 46
*See also* PURPLE N.K.V.D., 360, 368 Noise (in information
theory), 450^51 Nomenclators, xiv, 84, 87, 402, 427
death of, 112, 114 Nomura, T., 325 North Africa campaign, 239,
251-256 Norway, 242, 257-258, 259,
264 N.S.A. *See* National Security
Agency
Nsibidi script, 77 Null, definition, xii Null cipher, 281, 282-283,
293
Oberkommando der Kriegs-marine, 231, 241, 264
Oberkommando der Luftwaffe, 231, 240
Oberkommando der Wehr-
macht, 231-237 Oberkommando des Heeres,
231, 237 Occultism, 79 Oda, Lieutenant, 326 Office of Strategic Services,
273
Off-line encipherment, definition, 197
O.G.P.U., 361, 362 Ohnesorge, W., 296-298 *Oite. See* PA-K2 O.K.H. 231, 237 O.K.L. 231, 240 O.K.M. 231,
241, 264 O.K.W. 321-237 On-line encipherment, 197,
400 138th Radio Intelligence
Company 320-322 One-time pad, 216, 368, 371-
372, 388 One-time system (tape, pads),
199, 368 OP-16-F2, 13 OP-20-G, 1, 11-12, 13, 23, 26,
28, 193, 266, 269, 301, 303,
315
OP-20-cx, 13 OP-20-GY, 1, 2, 13 OP-20-GZ, 13 Open code, 281-283
ORANGE, 22
Oshima, H., 35, 273-274 O.S.S. *See* Office of Strategic
Services OVERLORD, 268 Ovid, 414 Ozaki, H., 327
PA-K2, 18-19, 38, 39, 40, 44,
45, 46, 66 Painvin, G. J., 159-165, 172,
301, 442 solution of ADFGX cipher,
159-160, 161, 442 Panin, N. P., 342

Parke, L. W., 13 Parker, R. T., 194, 197, 409 Paschke, A., 216, 218 "Passport code," 18 A "Pats," *See* microdot
T
Pearl Harbor attack, 1-68 *W*
378 f!
Pering, A. *V.,* 3, 13 **"
Pers z, 216-224, 230 Personal advertisements, 414-
415
Peter the Great, 341 ,
Petersen, T. C., 438 '%>' Petrov, E., 361 Petrov, V. M., 360-361 Phelippes, T., 86-88, 417 Philippines, U.S. Navy crypt-analytic unit, 12, 45, 301-
303
Pictures, encipherment of, 203 Pierce, E. C., 279-280, 286 Pigpen cipher, 413 Placode, definition, xiv Plaintext, definition, xi, xv Playfair cipher, 7, 118-121,
155, 328-330, 403 Playfair, L., 118, 120-121 Pletts, J. St. V., 187 Plutarch, 76 Poe, E. A., 416 Polk, F. L., 148-149 Pokorny, H., 350-352, 353,
356
Poland, 215
Polyalphabetic substitution, 350, 351, 353, 354
definition, xii
development of, 90-99
eclipse of, 99-100
rebirth of, 113
solution of, 123-124, 127-
128, 199-200 Polybius square, 76, 121, 343,
403
Polygrams, definition, xiii *Polygraphia libri sex,* 95 Polyphonic substitution, 415 Porta, G. B., 98
Postal Telegraph Cable Company, 203
Praun, A., 237
Price, B., 277, 279
Prisoners' cipher, 343-344
Private Office, 109
Probable word solutions, 441-442
PROD, 390
Prohibition, 420-422
Protocryptography, 72
*PT-109,* 328
PURPLE, 1-2, 15, 21-26, 42, 191, 266, 273-274, 315
Puzzle cryptograms, 411
Qalqashandi, 80-81
Rabelais, F., 416
Radar, 310
Radio, 153-165, 402
Radio Corporaation of America, 16, 39-40, 294
Radio intelligence, 9-10
Radio intelligence companies, 272, 320-321
Radio Intelligence Publications, 45
Radiotelephone. *See* Telephone secrecy
Random key, 199 quasi-random key, 401—402
Raven, F. A., 26, 390
R.C.A. *See* Radio Corporation of America
RED (Japanese), 15, 22, 23
Redman, J., 312
Redundancy, 444-450
Reichssicherheitshauptamt, 226-231
*Rendezvous* (film), 181-182
Rennenkampf, P., 345-350 *passim*
Ribbentrop, J. von, 216, 229
Rickert, E., 171
Rin-spuns, 77

Riverbank Laboratories, 185-
190 Riverbank Publications, 189-
190, 198
Robot cryptanalysts, 219, 236 Rochefort, J. J., 8, 37, 45, 300, 302, 303, 311
*See also* Combat Intelligence Unit Roehm, E., 225 Rogers, J. H., 291 Rohrbach, H., 217, 222 Rome, 77
Rommel, D. C. von, 250-252 Ronge, M., 227 Room 40, 130-133, 172, 263 Room 100, 256 Room 2646, 192
Roos, W. R., 282 Roosevelt, F. D., 29, 48-49,
50-51, 54-55, 57-58, 62-
63, 67, 295-296, 298 Rossignol, A., 101-104 Rote Kapelle, 368 Rotors, 204-205, 406
machines, 207, 209-210, 400
solution of, 191, 205-206
*See also* Damm; Enigma; Hebern; Koch; Scherbius Rotscheidt, W., 236 Rowlett, F. B., 11, 192, 400 R.S.H.A.
*See* Reichssicher-
heitshauptamt Rumrunners, 420-422 Running keys, 127, 199, 200 Russia, 129, 177, 395
black chambers, 341
Cold war, 371-377
cryptanalysis, 367-368
cryptosystems solved, 350-351, 353-356, 363-367
Czarist, 341-342
diplomatic cryptosystems, 368
military cryptosystems, 350, 351, 353, 354, 355-356, 362-363, 364
spy cryptosystems, 368-369,
371-372, 376-377 World War I, 344-357 World War II, 362-370
s code, 330-331
Safford, L. F., 11-12, 192-
193, 208, 269, 315 Samsonov, A., 346-349 Sandier, R., 259 Samoff, D., 16 Satake, T., 324, 327 Schapper,
Gottfried, 225 Schauffler, R., 216, 218, 224 Schellenberg, W., 227-228,
230, 298
Scherbius, A., 210, 329 Scherschmidt, H., 216 Schimpf, H., 225 Schlusselheft, 155-157, 159 Schutzstaffel
(S.S.), 225-226 Scientific method, 441 Scramblers, 290-298, 386, 423 S.D. *See* Sicherheitsdienst SEALION,
operation, 264-265 Secrecy, 452 Secret Office, 109 Seebohm, A., 253, 254 Segerdahl, E. O., 258, 260 Selchow,
K., 216, 218 Semagrams, 281, 283-284 Service du Chiffre, 163 Servizio Informazione Mili-
taire, 246-248 *passim* Servizio Informazione Segre-
to, 245
Sezione 5, 246-248 Sezione 6, 246, 247-248 Shakespeare-Bacon controversy, 184-185, 416, 459 Shannon, C. E.,
407, 443-451
*passim* Shaw, H. R., 279-280, 286
SHESHACH, 72
Shift registers, 402 Shimizu, Lieutenant, 326 *Shoho,* 304

Shungsky, 361 Siam, 77-78
Sicherheitsdienst, 225-226 Siemens & Halske machine, 237-238, 261-262
**SIGABA, 317**
Signal Intelligence, xv School, 11
Signal Security, xv
Signal Security Agency, 273, 274, 317-319
SIGTOT, 203
S. I. M. *See* Servizio Informa-zione Militaire
Sinkov, A., 192, 320, 329, 390
S.I.S. (Signal Intelligence Service), 2, 6,7, 11, 23, 25, 28,40,46,266,316-317
Skeat, W. W., 406
Skytale, 75-76
Smith, E. *See* Friedman, E. S.
Smith, F. O. J., 111-112
Smith, L. C., & Corona Typewriters, Inc., 214
Sonderdienst Dahlem, 217
Sorge, R., 368
Sorge ring, 368, 369
Soro, G., 83
Soudart, E. A., 159
Soviet Union. *See* Russia
Spain, 84, 357, 424--427
Speech codes, 289-292
Spets-Otdel, 359-362
Spy cipher, 386-370, 371-327, 373, 376
Square table, 95-96, 99, 100
S.S. *See* Schutzstaffel
Stark, H. F., 4
Statistics, 189-190, 331, 442 *See also* mathematics
"Steganographia," 432
Steganograms, 281-289
Steganography, xi, 274-289
Stein, K., 236
Stimson, H. L., 4, 6, 178, 183, 457
Straddling checkerboard, 357-359, 368, 376
Street, G., 39-40
Strip cipher. *See* CSP-642; M-
138
Strong, L. C., 437 *Subh al-a 'sha,* 80 Substitution
basic solution of, 82-83 compared with transposition, 404 definition, xi *See also* Monoalphabetic substitution; Polyalpha-betic substitution; Transposition Suetonius, 77 Suez crisis, 398-399 Superencipherment, definition, xiv
*See also* Enciphered code Superimposition. *See* Kerck-
hoflfs superimposition Svensson, E., 11 Sweden, 210, 256-263, 363-
364 SYKO, 240, 241
Tableaux, 95-96, 98-99 Tabula recta, 95-96 Tabulators. *See* computers and
tabulators Tannenberg, Battle of, 348-
349 T.D.S. *See* Time-division
scramble
Technical Operational Division, 279-280, 281, 286,
288
*Telconia,* 129
Telegraph, 111-114, 154-155 Telegraphic Japanese, 27 Telephone secrecy, 289-298, 423
*See* also Wiretapping Teletype Corporation, 210 Teletypewriter, 193-198, 237-
238
Terminology, 190-191 Thailand, 77-78

Thiele, F., 233, 236
13040 (German code), 137,
143, 144, 148 Thucydides, 76 Tibet, 77 Time, 453-454 Time-division scramble, 293 *Times, The* (London), 414-415 T.O.D. (Technical Operations
Division), 279-280, 281,
286, 288 (Togo, S., 30, 43^*4, 61 jTojo, H., 30-31, 43 fTokumu Han, 322-327 Tombstones, 412 Tomographic ciphers, 121-122 *Traicte des Chiffres,* 98 Traffic analysis, xv, 8-10, 232,
305-306, 321-322, 326-
327
Traffic volume, 317-318, 407 Transmission security, definition, xi Transposition, 80, 238, 413
compared with substitution, 404
defined, xii
*See also* Skytale; Substitution
Trithemius, J., 95-97 xsu. *See* J series Tsukikawa, S., 39 Tuchman, B. W., 458 Turkey, 219, 224, 228-229, 231, 248, 263
*U-158,* 269
17-505, 270-271
U-boats, 132-133, 243-244,
269-272 Unbreakable cipher, 199-202,
216, 388
Unicity distance, 450 Unicity point, 450 United States, 191, 379
Air Force 389, 400
Army, 15, 389
cryptosystems, security of,
389-390, 402
cryptosystems solved, 110, 221-222, 231, 238-239, 241, 248-256, 325, 332 Navy, 14, 315-316, 381, 389
*See also* A.F.S.A.; Army Security Agency; Code and Cipher Compilation Section; Code and Signal Section; Combat Intelligence Unit; Federal Communications Commission; FRUPAC; G.2 A.6; Mi-8; National Security Agency; OP-20-o; Radio intelligence companies; S.I.S.; Signal Security Agency: T.O.D. Univacs, 394 Uruk, 72
Van Deman, R. H., 168
Vatican, 91, 177, 224
Vatsyayana, 72
Venice, 83
Vernam, G. S., 193-203, 329
system, 193-198, 202-203,
406
Verne, J., 416 Video scramblers, 386 Viete, F., 84-86 Vigenere, B. de, 97-99 Vigenere cipher, 97-100, 403, 406, 415, 440 Vinay, E., 197 Voge, R. G., 331 Voice communications, 289-
298
Volapuk, 125 _ Volunteer Evaluation Office,
232
von der Osten, Ulrich, 276 von Feilitzen, O., 258 von Neumann, J., 451 Voynich, E., 439

Voynich manuscript, 428-
439
Voynich, W., 432, 439 Vries, M. de, 440, 452
Waberski, P., 171 Walsingham, Sir Francis, 86-
89 Wanderer Werke machine,
237
Warburg, C. G., 257 Washington Disarmament
Conference, 175-177 Wave-form modification, 293 Weather-forecast codes, Japanese, 42, 322
Wehrmachtnachrichtenver-
bindungen, 232-233 Welker, G. W., 13 Wendland, V., 236 Wesemann, 243 Wheatstone, C., 117-118, 121,
415 Wheatstone cryptograph, 118,
187
Wigg, G., 398 Wilkins, J., 438 Willes, E., and family, 106-
108, 111, 113 Willoughby, C. A., 378 Wilson, Woodrow, 137-138,
140-141, 145, 153, 168 Winds code, 31-32, 34-35,
42-43
Wiretapping, 289 Witzke, L., 171 W.N.V. *See* Wehrmachtnach-
richtenverbindungen Wobble scramble, 293-294 Wolfe, J. R., 458 Women's Army Corps, 313 Woodward, F. C., 45,
300 World War I, 129-167, 168-
172, 186-188, 344-357
World War H, 1-68, 214-340,
362-370 Wright, W. A., 45, 300, 302,
310-311, 333
"Wurlitzer Organ," 286-287 Yale University, 439 Yamamoto, I., 7, 299-300,
308, 314
assassination, 332-338 Yamanashi, 327 *Yamato,* 331-332 Yardley, H. O., 167-168,
172-173, 181-183 *American Black Chamber,*
*The,* 30, 179-181 characteristics, 167-168 chief of American Black
Chamber, 6, 173-180 chief of Mi-8, 168-172 in China, 182-183, 323 interest in cryptology, 167-
169
"Japanese Diplomatic Secrets," 181 later life, 182-183 solves Japanese codes, 173-
177
Voynich manuscript, 433 "Yardley symptom," 168 Yezidis, 77
Yoshikawa, 15, 39, 44-45, 49 YU, 175-176 Yugoslavia, 246-247
Zacharias, E. M., 192-193 Zapp, Prof., 288 Zenith Radio Corporation, 0075 (German code), 134,
137, 139, 140, 142, 143,
145, 148
Ziegenriiger, J., 218-219 Zim, H. S., 458 Zimmermann telegram, 134-
153, 263 Zipf, G. K., 445

**THE HISTORY OF SECRET CODES— AND THE MEN WHO HAVE CREATED AND BROKEN THEM WITH DRAMATIC CONSEQUENCES FOR THE WORLD!**

"THRILLING!"
-CINCINNATI ENQUIRER
"A LAVISH, NOTABLE ACHIEVEMENT!"
-THE NEW YORK TIMES
-.-THE CLASSIC IN ITS FIELD!"
-CLIFTON FADIMAN, BOOK-OF-THE-MONTH CLUB NEWS

"Comprehensive and astounding ... utterly fascinating

to anyone interested in political or military history, mathematics, mystery or pure who-dun-it—
Beginning wii
hieroglyphics and ending with computers, David Kahn
has produced an anthology of a hundred detective stories,
one more ingenious than the last, and all real> central
to the fate of armies and kingdoms.
-THE WASHINGTON POST
"SUCH FASCINATION THAT THE READER MAY FIND
HIMSELF NEGLECTING HIS WORK, BEING LATE
TO DINNER, AND UNABLE TO GET TO BED AT A
REASONABLE HOUR."
-NEWSWEEK
SELECTED BY THE BOOK-OF-THE-MONTH CLUB
NEW AMERICAN LIBRARY PUBLISHES SIGNET, SIGNETTE, MENTOR, CLASSIC, PLUMES NAL BOOKS

---

[1] Not the same thing as the American name J for the J series of Japanese codes.

[2] Whence, apparently, its codename. In American prewar military and naval parlance, the codeword ORANGE meant *Japan* in official papers such as war plans, and even in personal letters between high-ranking officers. In the 1930s, Lieutenant Jack S. Holtwick, Jr., a Navy cryptanalyst, built a machine to solve a Japanese diplomatic cipher that was abandoned in 1938. American cryptanalysts could very naturally have called it the ORANGE machine. As the successors of this system appeared, each increasingly enigmatic, their American codenames might well have progressively deepened in hue.

[3] This is the literal translation made by Mr. Cory of GZ and given in MAGIC. But Friedman and others have contended that it does not take into account the Japanese tendency to speak in circumlocution and by indirection. The spirit of it might better be rendered into English, Friedman suggested, as "on the brink of catastrophe" or "on the verge of disaster." Kramer conceded that the words should not be interpreted as mildly as the English seems to indicate, but could imply "relations are reaching a crisis." The British translated this phrase as "Relations between Japan and (name of country) are extremely critical."

[4] This may be why Rochefort did not simply request the keys from Washington via the special monitors' channel.

[5] The correct plaintexts were simply *and,* with the extra *nd* probably an inadvertent repetition, and *China, it must,* with the LYL probably a codeword for *comma.*